(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－15373

(43)公開日　平成11年(1999)１月22日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｇ０９Ｃ　1/00	６２０	Ｇ０９Ｃ　1/00	６２０Ｚ
	６３０		６３０Ａ
			６３０Ｆ
	６４０		６４０Ｂ
			６４０Ｄ

審査請求　未請求　請求項の数35　ＯＬ　（全 31 頁）　最終頁に続く

(21)出願番号　特願平9－164506

(22)出願日　平成９年(1997)６月20日

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂二丁目17番22号

(72)発明者　青木　隆一
神奈川県川崎市高津区坂戸３丁目２番１号　ＫＳＰ　Ｒ&Ｄビジネスパークビル　富士ゼロックス株式会社内

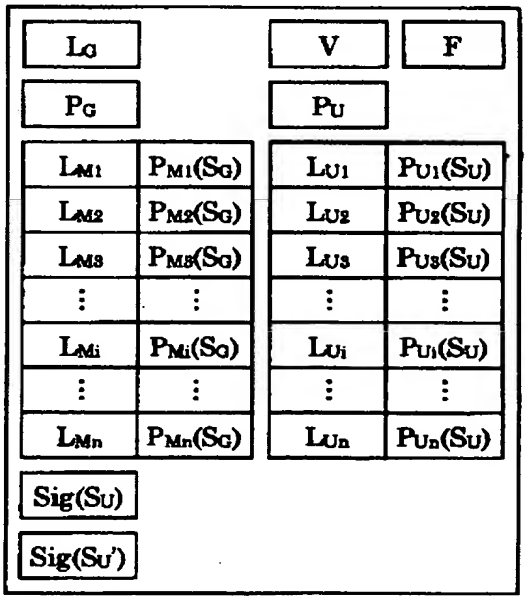
(74)代理人　弁理士　澤田　俊夫

(54)【発明の名称】　公開鍵暗号方式

(57)【要約】

【課題】　公開鍵暗号方式において、グループの概念を導入し、グループ内での情報の共有化およびグループ外に対する機密性を保持しながら、グループに属するメンバによる情報の暗号化および復号処理、グループ構成メンバの変更を可能とする。

【解決手段】　複数のメンバを構成員とするグループを単位とする公開鍵と秘密鍵の対を生成してグループに割り当てる。グループのメンバ固有の公開鍵により、グループの秘密鍵をそれぞれ暗号化し、それを一体化したグループ錠を形成する。グループの秘密鍵を利用する際には、メンバ固有の秘密鍵によって暗号化されたグループ秘密鍵を復号する。グループのメンバ変更に際しては、新しいバージョンのグループ錠を作り直すことにより対応する。また、グループの変更権所有者用の公開鍵と秘密鍵の対を生成し、変更権所有者用の秘密鍵によって新しいバージョンのグループ錠全体へ電子署名を施すことにより、グループ錠の変更の正当性を保証する。



【特許請求の範囲】

【請求項１】　平文を暗号化するデータ変換のために用いられる第１の鍵Ｐと、該第１の鍵と異なる鍵であり暗号を復号し平文とするデータ変換のために用いられる第２の鍵Ｓとの組み合わせによって構成される公開鍵暗号方式において、

１以上のメンバＭｉ（ｉ＝１～ｎ）を構成員とするグループを単位として割り当てられるグループ公開鍵P_Gおよびグループ秘密鍵S_Gと、

前記メンバＭｉに固有の公開鍵P_{Mi}の各々によって、前記グループ秘密鍵S_Gのデータ変換を実行し暗号化された１以上の暗号化グループ秘密鍵P_{Mi}（S_G）（ｉ＝１～ｎ）とを有し、

前記メンバＭｉ各々に固有のメンバ秘密鍵S_{Mi}による前記暗号化グループ秘密鍵P_{Mi}（S_G）の復号によって前記グループ秘密鍵S_Gを獲得し、該獲得した前記グループ秘密鍵S_Gを使用して、前記グループ公開鍵P_Gによって暗号化された暗号情報の復号を実行するように構成したことを特徴とする公開鍵暗号方式。

【請求項２】　前記暗号化された暗号情報が、他の暗号情報の復号鍵Ｓ１であり、

前記メンバＭｉ各々に固有のメンバ秘密鍵S_{Mi}による前記暗号化グループ秘密鍵P_{Mi}（S_G）の復号によって前記グループ秘密鍵S_Gを獲得し、前記グループ公開鍵P_Gによって暗号化された前記復号鍵Ｓ１であるP_G（Ｓ１）を、前記グループ秘密鍵S_Gにより復号することにより前記復号鍵Ｓ１を獲得し、前記他の暗号情報の復号を該獲得した前記復号鍵Ｓ１によって実行する構成としたことを特徴とする請求項１記載の公開鍵暗号方式。

【請求項３】　前記メンバＭｉの各々は、個人、複数の個人から形成されるグループ、あらかじめ設定された役割の実行機能、およびあらかじめ設定された役割の実行システムのいずれかを識別する識別子であることを特徴とする請求項１または２記載の公開鍵暗号方式。

【請求項４】　前記グループを単位として生成されるグループ公開鍵P_Gおよび前記暗号化グループ秘密鍵P_{Mi}（S_G）（ｉ＝１～ｎ）の組は複合鍵として構成されることを特徴とする請求項１乃至３いずれかに記載の公開鍵暗号方式。

【請求項５】　前記複合鍵は、

複合鍵の正当な変更権所有者に帰属する複合鍵変更公開鍵P_Uと、該複合鍵変更公開鍵P_Uと対をなす複合鍵変更秘密鍵S_Uを該複合鍵の変更を行う権利を有するメンバ固有の公開鍵P_{Ui}によるデータ変換によって暗号化した１以上の暗号化複合鍵変更秘密鍵P_{Ui}（S_U）を有することを特徴とする請求項４に記載の公開鍵暗号方式。

【請求項６】　前記複合鍵における前記グループ公開鍵P_Gとグループ秘密鍵S_Gとの対は、該複合鍵の構成の変更に応じて変更されることを特徴とする請求項４または５記載の公開鍵暗号方式。

【請求項７】　前記複合鍵変更公開鍵P_Uおよび複合鍵変更秘密鍵S_Uは、該複合鍵の変更権所有者の変更により、新たな複合鍵変更公開鍵P_Uおよび複合鍵変更秘密鍵S_Uの対に置き換えられることを特徴とする請求項５または６に記載の公開鍵暗号方式。

【請求項８】　前記複合鍵は、該複合鍵を構成するデータに対し前記複合鍵変更秘密鍵S_Uにより電子署名を実行した電子署名ブロックを有することを特徴とする請求項５乃至７いずれかに記載の公開鍵暗号方式。

【請求項９】　変更された複合鍵を構成するデータに対し前記複合鍵変更秘密鍵S_Uにより電子署名した結果である署名ブロックを前記変更された複合鍵を構成するデータに新たに付与し、該署名ブロックを含めたデータを新たな複合鍵とし、該新たな複合鍵に対して前記複合鍵変更前の変更用秘密鍵S_U'で署名した第２の署名ブロックを有することを特徴とする請求項８記載の公開鍵暗号方式。

【請求項１０】　前記複合鍵は、

該複合鍵のバージョンを示すバージョン識別子Ｖを有し、

該バージョン識別子Ｖは、該複合鍵が最新バージョンであるか否かを示すことを特徴とする請求項４乃至９いずれかに記載の公開鍵暗号方式。

【請求項１１】　前記複合鍵は、

前バージョン扱い識別子Ｆを有し、

該前バージョン扱い識別子Ｆは、該複合鍵の直前のバージョンの取り扱いについて規定するものであることを特徴とする請求項４乃至１０いずれかに記載の公開鍵暗号方式。

【請求項１２】　前記前バージョン扱い識別子Ｆは、前記複合鍵の変更内容に基づいて生成されることを特徴とする請求項１１記載の公開鍵暗号方式。

【請求項１３】　前記前バージョン扱い識別子Ｆは、前記複合鍵の変更の遡及的適用の有無を識別する情報を含むことを特徴とする請求項１１または１２記載の公開鍵暗号方式。

【請求項１４】　少なくとも平文を共通鍵Ｋにより暗号化した暗号情報Ｋ（Ｄ）と、１以上のメンバＭｉ（ｉ＝１～ｎ）を構成員とするグループに属するメンバ個々の公開鍵Ｐｉによって前記共通鍵Ｋを暗号化した１以上のＰｉ（Ｋ）とを有する構成データを暗号情報として構成したことを特徴とする公開鍵暗号方式。

【請求項１５】　平文を暗号化するデータ変換のために用いられる第１の鍵と、該第１の鍵と異なる鍵であり、暗号を復号し平文とするデータ変換のために用いられる第２の鍵との組み合わせによって構成される公開鍵暗号方式における暗号化装置において、

１以上のメンバＭｉ（ｉ＝１～ｎ）を構成員とするグループを単位として割り当てられるグループ公開鍵P_Gを用いて平文をデータ変換することにより、暗号化する暗

号化手段と、
前記メンバＭｉの公開鍵P_{Mi}によって前記グループを単位として割り当てられるグループ秘密鍵S_Gをデータ変換し暗号化することにより、１以上の暗号化グループ秘密鍵P_{Mi}（S_G）（ｉ－１～ｎ）を生成する暗号化秘密鍵生成手段と、を有することを特徴とする暗号化装置。
【請求項１６】　グループ単位毎に公開鍵と秘密鍵とを生成する鍵生成手段を有し、
該鍵生成手段が生成した公開鍵および秘密鍵を前記グループ公開鍵P_Gとグループ秘密鍵S_Gとして割り当てることを特徴とする請求項１５記載の暗号化装置。
【請求項１７】　前記グループ公開鍵P_Gにより暗号化された前記暗号情報に対して、該暗号化を実行するメンバまたは該メンバが属するグループの秘密鍵を適用して署名した電子署名ブロックと該適用した秘密鍵の公開鍵とを含む署名情報を生成することを特徴とする請求項１５または１６に記載の暗号化装置。
【請求項１８】　自己の使用可能なグループ公開鍵または個人公開鍵の少なくともいずれか一方を含む公開錠リストを有し、該公開錠リストから選択した暗号の復号を可能とするメンバＭｉの公開鍵P_{Mi}を用いて前記グループ秘密鍵S_Gのデータ変換による１以上の暗号化グループ秘密鍵P_{Mi}（S_G）（ｉ＝１～ｎ）を生成することを特徴とする請求項１５乃至１７いずれかに記載の暗号化装置。
【請求項１９】　１以上のメンバＮｊ（ｊ＝１～ｍ）を構成員とするグループを単位として生成されるグループ公開鍵P_Cおよびグループ秘密鍵S_Cと、前記メンバＮｊに固有の公開鍵P_{Nj}の各々によって前記グループ秘密鍵S_Cのデータ変換を実施して暗号化された１以上の暗号化グループ秘密鍵P_{Nj}（S_C）（ｊ＝１～ｍ）とを構成要素として有する複合錠のグループ公開鍵P_Cを前記公開錠リストが含む場合において前記複合錠の変更に応じて前記公開錠リストを更新する手段を有することを特徴とする請求項１８に記載の暗号化装置。
【請求項２０】　平文を暗号化するデータ変換のために用いられる第１の鍵と、該第１の鍵と異なる鍵であり暗号を復号し平文とするデータ変換のために用いられる第２の鍵との組み合わせによって構成される公開鍵暗号方式における復号装置において、
暗号文の復号に用いる復号鍵Ｓを暗号の受け手の公開鍵Ｐｊで暗号化した暗号化秘密鍵Ｐｊ（Ｓ）を自己またはグループの秘密鍵Ｓｊにより復号する秘密鍵復号手段と、
前記秘密鍵復号手段により復号し、獲得した復号鍵Ｓにより、前記暗号文を復号する復号手段と、
を備えたことを特徴とする復号装置。
【請求項２１】　前記暗号化された暗号情報が、他の暗号情報の復号鍵Ｓ１であり、
前記復号手段により獲得した前記復号鍵Ｓ１によって前記他の暗号情報の復号を実行する手段を有することを特徴とする請求項２０記載の復号装置。
【請求項２２】　１以上のメンバＮｊ（ｊ＝１～ｍ）を構成員とするグループを単位として生成されるグループ公開鍵P_Cおよびグループ秘密鍵S_Cと、前記メンバＮｊに固有の公開鍵P_{Nj}の各々によって前記グループ秘密鍵S_Cのデータ変換を実施して暗号化された１以上の暗号化グループ秘密鍵P_{Nj}（S_C）（ｊ＝１～ｍ）とを構成要素として有する複合錠の前記暗号化グループ秘密鍵P_{Nj}（S_C）（ｊ＝１～ｍ）から自己の秘密鍵S_{Nj}により前記グループ秘密鍵S_Cを復号し、前記秘密鍵復号手段は該復号したグループ秘密鍵S_Cを用いて前記復号鍵Ｓを獲得することを特徴とする請求項２０または２１に記載の復号装置。
【請求項２３】　前記秘密鍵復号手段によって復号したグループ秘密鍵S_{C1}を用いて他の複合錠における暗号化グループ秘密鍵からグループ秘密鍵S_{C2}を復号する操作を再帰的に行う再帰的実行手段と、
前記再帰的実行手段により復号したグループ秘密鍵を適用することにより、暗号化された「暗号情報の復号鍵」を復号する手段を有することを特徴とする請求項２２に記載の復号装置。
【請求項２４】　前記復号装置は、暗号文を復号するデータ変換の際に使用する秘密錠リストを有し、
該秘密錠リストは、自己の秘密鍵を用いて復号することにより獲得可能な複合錠を登録したリストであることを特徴とする請求項２０乃至２３いずれかに記載の復号装置。
【請求項２５】　前記秘密錠リスト中に含まれる複合錠には、自己の秘密鍵により直接的に復号鍵を得ることが可能な個人錠と、
自己の秘密鍵の適用により暗号化秘密鍵を復号し、間接的に復号鍵を得ることが可能なグループ錠とが区分されていることを特徴とする請求項２４に記載の復号装置。
【請求項２６】　新たに取得した複合錠が有するバージョン扱い識別子Ｆに基づいて、前記秘密錠リストの内容を更新する手段を有することを特徴とする請求項２４または２５に記載の復号装置。
【請求項２７】　平文を暗号化するデータ変換のために用いられる第１の鍵と、該第１の鍵と異なる鍵であり、暗号を復号し平文とするデータ変換のために用いられる第２の鍵との組み合わせによって構成される公開鍵暗号方式における暗号化方法において、
１以上のメンバＭｉ（ｉ＝１～ｎ）を構成員とするグループを単位として生成されるグループ公開鍵P_Gを用いて平文をデータ変換することにより、暗号化するステップと、
前記メンバＭｉの公開鍵P_{Mi}によって前記グループを単位として生成されるグループ秘密鍵S_Gをデータ変換し暗号化することにより、１以上の暗号化グループ秘密鍵

P_{Mi}（S_G）（i＝1～n）を生成するステップと、
を有することを特徴とするグループ公開鍵暗号方式における暗号化方法。

【請求項28】　平文を暗号化するデータ変換のために用いられる第1の鍵と、該第1の鍵と異なり、暗号を復号し平文とするデータ変換のために用いられる第2の鍵との組み合わせによって構成される公開鍵暗号方式における復号方法において、
1以上のメンバMi（i＝1～n）を構成員とするグループを単位として生成されるグループ秘密鍵S_Gの前記メンバの公開鍵P_{Mi}による暗号化により生成された暗号化グループ秘密鍵P_{Mj}（S_G）を前記メンバの秘密鍵S_{Mi}によって復号し、前記グループ秘密鍵S_Gを獲得するステップと、
前記グループを単位として生成されるグループ公開鍵P_Gにより暗号化された情報を、前記獲得されたグループ秘密鍵S_Gを用いてデータ変換することにより暗号化情報を復号するステップと、
を有することを特徴とする公開鍵暗号方式における復号方法。

【請求項29】　平文を暗号化するデータ変換のために用いられる第1の鍵と、該第1の鍵と異なり、暗号を復号し平文とするデータ変換のために用いられる第2の鍵との組み合わせによって構成される公開鍵暗号方式であり、1以上のメンバMi（i＝1～n）を構成員とするグループを単位として生成されるグループ公開鍵P_Gおよびグループ秘密鍵S_Gと、前記メンバMiに固有の公開鍵P_{Mi}の各々によって、前記グループ秘密鍵S_Gのデータ変換を実行し暗号化された1以上の暗号化グループ秘密鍵P_{Mi}（S_G）（i＝1～n）とを構成要素として有する複合錠を使用する公開鍵暗号方式における複合錠の生成方法であって、
1以上のメンバMi（i＝1～n）を構成員とするグループを単位として公開鍵P_Gと秘密鍵S_Gとを生成するステップと、
前記メンバMiに固有の公開鍵P_{Mi}の各々によって、前記生成されたグループ秘密鍵S_Gのデータ変換を実行し暗号化された1以上の暗号化グループ秘密鍵P_{Mi}（S_G）（i＝1～n）を生成するステップと、
複合錠の変更を制御する複合錠変更秘密鍵S_Uを、変更を行う権利を有するメンバ固有の公開鍵P_{Ui}によるデータ変換によって暗号化された1以上の暗号化複合錠変更秘密鍵P_{Ui}（S_U）を生成するステップと、
前記生成された公開鍵P_G、暗号化グループ秘密鍵P_{Mi}（S_G）および暗号化複合錠変更秘密鍵P_{Ui}（S_U）とを含むデータに対して前記生成された複合錠変更秘密鍵S_Uを用いて電子署名を行うステップと、を有することを特徴とする複合錠の生成方法。

【請求項30】　平文を暗号化するデータ変換のために用いられる第1の鍵と、該第1の鍵と異なり、暗号を復号し平文とするデータ変換のために用いられる第2の鍵との組み合わせによって構成される公開鍵暗号方式であり、1以上のメンバMi（i＝1～n）を構成員とするグループを単位として生成されるグループ公開鍵P_Gおよびグループ秘密鍵S_Gと、前記メンバMiに固有の公開鍵P_{Mi}の各々によって、前記グループ秘密鍵S_Gのデータ変換を実行し暗号化された1以上の暗号化グループ秘密鍵P_{Mi}（S_G）（i＝1～n）と、複合錠の変更を制御する複合錠変更秘密鍵S_Uを、変更を行う権利を有するメンバ固有の公開鍵P_{Ui}によるデータ変換によって暗号化された1以上の暗号化複合錠変更秘密鍵P_{Ui}（S_U）とを構成要素として有する複合錠を使用する暗号化方式における複合錠の変更方法であって、
複合錠の内容を変更するステップと、
前記暗号化複合錠変更秘密鍵P_{Ui}（S_U）から自己の秘密鍵S_{Ui}を用いて復号することにより複合錠変更秘密鍵S_Uを得るステップと、
前記公開鍵P_G、暗号化グループ秘密鍵P_{Mi}（S_G）および暗号化複合錠変更秘密鍵P_{Ui}（S_U）とを含むデータに対して前記生成された複合錠変更秘密鍵S_Uを用いて電子署名を行うステップと、を有することを特徴とする複合錠の変更方法。

【請求項31】　複合錠の変更を制御する複合錠変更公開鍵P_Uおよび複合錠変更秘密鍵S_Uの新たなペアを生成するステップと、
前記複合錠の変更を行う権利を有するメンバ固有の公開鍵P_{Ui}によるデータ変換によって暗号化した1以上の暗号化複合錠変更秘密鍵P_{Ui}（S_U）を生成し、複合錠に付与するステップと、
を有することを特徴とする請求項30記載の公開鍵暗号方式における複合錠の変更方法。

【請求項32】　変更された複合錠を構成するデータに対し前記複合錠変更秘密鍵S_Uにより電子署名した結果である署名ブロックを前記変更された複合錠を構成するデータに新たに付与し、該署名ブロックを含めた全体を新たな複合錠とし、該新たな複合錠に対して前記複合錠変更前の変更用秘密鍵S_Uで署名するステップを有することを特徴とする請求項31記載の公開鍵暗号方式における複合錠の変更方法。

【請求項33】　平文を暗号化するデータ変換のために用いられる第1の鍵と、該第1の鍵と異なり、暗号を復号し平文とするデータ変換のために用いられる第2の鍵との組み合わせによって構成される公開鍵暗号方式であり、1以上のメンバMi（i＝1～n）を構成員とするグループを単位として生成されるグループ公開鍵P_Gおよびグループ秘密鍵S_Gと、前記メンバMiに固有の公開鍵P_{Mi}の各々によって、前記グループ秘密鍵S_Gのデータ変換を実行して暗号化された1以上の暗号化グループ秘密鍵P_{Mi}（S_G）（i＝1～n）とを構成要素として有する複合錠を使用する公開鍵暗号方式における複合

錠変更方法において、
メンバの変更が現時点以降の変更である場合は、新たなグループ公開鍵P_Gと新たなグループ秘密鍵S_Gとのペアを生成し、該複合錠の新たな公開鍵および秘密鍵として用い、
メンバの変更が過去に溯る変更の場合には、現在のグループ公開鍵P_Gとグループ秘密鍵S_Gとのペアをそのまま継続して該複合錠の公開鍵および秘密鍵として用いることを特徴とする公開鍵暗号方式における複合錠の変更方法。
【請求項34】　平文を暗号化するデータ変換のために用いられる第1の鍵と、該第1の鍵と異なる鍵であり、暗号を復号し平文とするデータ変換のために用いられる第2の鍵との組み合わせによって構成される公開鍵暗号方式における暗号化方法を記録したコンピュータ読み取り可能な記録媒体において、
1以上のメンバMi（i＝1～n）を構成員とするグループを単位として生成されるグループ公開鍵P_Gを用いて平文をデータ変換することにより、暗号化するステップと、
前記メンバMiの公開鍵P_{Mi}によって前記グループを単位として生成されるグループ秘密鍵S_Gをデータ変換し暗号化することにより、1以上の暗号化グループ秘密鍵P_{Mi}（S_G）（i＝1～n）を生成するステップと、
を実行するプログラムを記録したコンピュータ読み取り可能な記録媒体。
【請求項35】　平文を暗号化するデータ変換のために用いられる第1の鍵と、該第1の鍵と異なり、暗号を復号し平文とするデータ変換のために用いられる第2の鍵との組み合わせによって構成される公開鍵暗号方式における復号方法を記録したコンピュータ読み取り可能な記録媒体において、
1以上のメンバMi（i＝1～n）を構成員とするグループを単位として生成されるグループ秘密鍵S_Gの前記メンバの公開鍵P_{Mi}による暗号化により生成された暗号化グループ秘密鍵P_{Mi}（S_G）を前記メンバの秘密鍵S_{Mi}によって復号し、前記グループ秘密鍵S_Gを獲得するステップと、
前記グループを単位として生成されるグループ公開鍵P_Gにより暗号化された情報を、前記獲得されたグループ秘密鍵S_Gを用いてデータ変換することにより暗号化情報を復号するステップと、
を実行するプログラムを記録したコンピュータ読み取り可能な記録媒体。
【発明の詳細な説明】
【0001】
【発明の属する技術分野】本発明は、平文を暗号化するデータ変換のために用いられる第1の鍵と、第1の鍵と異なり暗号を解読し平文とするデータ変換のために用いられる第2の鍵との組み合わせによって構成される公開鍵暗号方式に関し、特に公開鍵暗号方式において、グループの概念を導入し、グループに属する任意のメンバによる平文の暗号化処理、および暗号の復号処理をグループを単位として生成されたグループ鍵を用いることによって実行し、グループ内と外との間では高度な機密性を保ちながら、グループ内のメンバ間では、メンバであることの確認の基に暗号を復号することを可能とし、また、グループに属するメンバはグループとしての電子署名を行うことを可能とした公開鍵暗号方式に関する。
【0002】
【従来の技術】公開鍵暗号と呼ばれる暗号方式が米国特許4，200，700号に記載されている。公開鍵暗号は、平文を暗号化する際に用いる公開鍵と、暗号を平文に復号する際に用いる秘密鍵とを有する。公開鍵と秘密鍵とは異なる鍵であり、公開鍵は、文字通り公開され、公知の状態においておくことが可能である。従来の暗号方式は、暗号化および復号に同一の鍵が使用されており、暗号化の際の鍵の機密性を保つことが重要な課題であったが、この公開鍵暗号方式では、暗号化の鍵の機密性は不要となる。また、暗号文書を通信する人数がn人であった場合、従来の暗号化、復号共通鍵方式であるとn×（n－1）÷2個の鍵が必要となるが、公開鍵暗号方式ではn個の鍵で済むといった利点がある。また、各人の署名、すなわち各人による秘密鍵による暗号化処理においても同じ枠組みを用いることができるといった特徴がある。例えば秘密鍵Aを有する暗号通信メンバPが、通信文Xを秘密鍵Aで変換し、変換した文書Yと通信文Xを他のメンバQに送付し、メンバQは、メンバPの公開鍵Bで変換文書Yを変換し、Yの変換結果がXと一致すれば、その文書は、確かにメンバPによって送付されたものであることが確認できる。このように公開鍵暗号方式には、従来の暗号方式には無いいくつかの優れた点を有する。
【0003】また、特開平7－297818号公報に、グループに対する公開鍵と秘密鍵の割り当てについての構成が記載されている。これは、カードのような物理的実態にグループ秘密鍵を埋め込み、カードをグループのメンバが確実に所持することを前提としたシステムである。すなわち、上述の秘密鍵と公開鍵の暗号システムをカードという実態を利用した構成とすることによって、個人という恒久的な存在から分離したカードという物理的実態を利用して鍵の管理を実現している。
【0004】
【発明が解決しようとする課題】公開鍵暗号方式では、個人のような恒久的な存在を独立した単位として設定している。従って、個人以外の例えば複数のメンバを一つの単位として設定する必要がある場合等には十分な機能を果たし得ない。また、上述のようなカードを使用したシステムにおいては、カードというハードウェアを用いなければならないこと、カード自体の管理の問題、カー

ドの紛失、盗難等に起因するカード所有者の正当性の問題、すなわちカード保有者がカードの正当な所有者であるかどうかの判断が困難であるという問題が発生する。

【０００５】例えば、企業のように、部、課、あるいは係といった組織は協同作業単位であり、またそのような組織とは独立に成り立つタスクフォースといった複数の個人から構成される協同作業単位である。これら協同作業単位では、情報も共有される必要がある。すなわち、協同作業単位の内部と外部との関係では、情報の機密性を維持する必要があるが、内部の各メンバ間での情報の流通は必要となる。従って、その協同作業単位の任意の構成員が共有情報に対する復号処理、あるいは署名処理を行えるような暗号方式が必要となる。

【０００６】さらに、協同作業単位の構成員は追加や削除といった変更が発生することがあるため、暗号方式は、これら構成員の変更にも対応可能な方式であることが必要である。また、協同作業単位と同様に、企業内における人事部長のような役割を果たすために、ある時点においてその役割を果たしている特定の個人とは独立な、すなわちその役割を果たしている個人の変更に対応可能な形で、その役割に応じた特定かつ継続的な機密状態を保持する必要がある。

【０００７】本発明は上記の問題を解決する暗号方式を提供する。本発明は、公開鍵暗号方式を個人を単位とするのではなく、個人およびグループを要素とする集合であるグループにおいて使用可能とし、特定のグループに属する構成員（メンバ）が復号可能な暗号化方式を提供することを目的とする。

【０００８】さらに本発明は、特定のグループに属する任意のメンバによる署名を可能とし、署名された文書がその特定グループに属するメンバによる署名であることを確認することが可能な署名方式を提供する。

【０００９】

【課題を解決するための手段】本発明の公開鍵暗号方式は、平文を暗号化するデータ変換のために用いられる第１の鍵Ｐと、該第１の鍵と異なる鍵であり暗号を復号し平文とするデータ変換のために用いられる第２の鍵Ｓとの組み合わせによって構成される公開鍵暗号方式において、１以上のメンバＭｉ（ｉ＝１～ｎ）を構成員とするグループを単位として割り当てられるグループ公開鍵P_GおよびS_Gと、前記メンバＭｉに固有の公開鍵P_{Mi}の各々によって、前記グループ秘密鍵S_Gのデータ変換を実行し暗号化された１以上の暗号化グループ秘密鍵$P_{Mi}(S_G)$（ｉ＝１～ｎ）とを有し、前記メンバＭｉ各々に固有のメンバ秘密鍵S_{Mi}による前記暗号化グループ秘密鍵$P_{Mi}(S_G)$の復号によって前記グループ秘密鍵S_Gを獲得し、該獲得した前記グループ秘密鍵S_Gを使用して、前記グループ公開鍵P_Gによって暗号化された暗号情報の復号を実行するように構成したことを特徴とする。

【００１０】また、本発明の公開鍵暗号方式は、前記暗号化された暗号情報が、他の暗号情報の復号鍵Ｓ１であり、前記メンバＭｉ各々に固有のメンバ秘密鍵S_{Mi}による前記暗号化グループ秘密鍵$P_{Mi}(S_G)$の復号によって前記グループ秘密鍵S_Gを獲得し、前記グループ公開鍵P_Gによって暗号化された前記復号鍵Ｓ１である$P_G(S1)$を、前記グループ秘密鍵S_Gにより復号することにより前記復号鍵Ｓ１を獲得し、前記他の暗号情報の復号を該獲得した前記復号鍵Ｓ１によって実行する構成としたことを特徴とする。

【００１１】また、本発明の公開鍵暗号方式において、前記メンバＭｉの各々は、個人、複数の個人から形成されるグループ、あらかじめ設定された役割の実行機能、およびあらかじめ設定された役割の実行システムのいずれかを識別する識別子であることを特徴とする。

【００１２】また、本発明の公開鍵暗号方式において、前記グループを単位として生成されるグループ公開鍵P_Gおよび前記暗号化グループ秘密鍵$P_{Mi}(S_G)$（ｉ＝１～ｎ）の組は複合錠として構成されることを特徴とする。

【００１３】また、本発明の公開鍵暗号方式において、前記複合錠は、複合錠の正当な変更権所有者に帰属する複合錠変更公開鍵P_Uと、該複合錠変更公開鍵P_Uと対をなす複合錠変更秘密鍵S_Uを該複合錠の変更を行う権利を有するメンバ固有の公開鍵P_{Ui}によるデータ変換によって暗号化した１以上の暗号化複合錠変更秘密鍵$P_{Ui}(S_U)$を有することを特徴とする。

【００１４】また、本発明の公開鍵暗号方式において、前記複合錠における前記グループ公開鍵P_Gとグループ秘密鍵S_Gとの対は、該複合錠の構成の変更に応じて変更されることを特徴とする。

【００１５】また、本発明の公開鍵暗号方式において、前記複合錠変更公開鍵P_Uおよび複合錠変更秘密鍵S_Uは、該複合錠の変更権所有者の変更により、新たな複合錠変更公開鍵P_Uおよび複合錠変更秘密鍵S_Uの対に置き換えられることを特徴とする。

【００１６】また、本発明の公開鍵暗号方式において、前記複合錠は、該複合錠を構成するデータに対し前記複合錠変更秘密鍵S_Uにより電子署名を実行した電子署名ブロックを有することを特徴とする。

【００１７】また、本発明の公開鍵暗号方式は、変更された複合錠を構成するデータに対し前記複合錠変更秘密鍵S_Uにより電子署名した結果である署名ブロックを前記変更された複合錠を構成するデータに新たに付与し、該署名ブロックを含めたデータを新たな複合錠とし、該新たな複合錠に対して前記複合錠変更前の変更用秘密鍵S_U'で署名した第２の署名ブロックを有することを特徴とする。

【００１８】また、本発明の公開鍵暗号方式において、前記複合錠は、該複合錠のバージョンを示すバージョン

識別子Ｖを有し、該バージョン識別子Ｖは、該複合鍵が最新バージョンであるか否かを示すことを特徴とする。

【００１９】また、本発明の公開鍵暗号方式において、前記複合鍵は、前バージョン扱い識別子Ｆを有し、該前バージョン扱い識別子Ｆは、該複合鍵の直前のバージョンの取り扱いについて規定するものであることを特徴とする。

【００２０】また、本発明の公開鍵暗号方式において、前記前バージョン扱い識別子Ｆは、前記複合鍵の変更内容に基づいて生成されることを特徴とする。

【００２１】また、本発明の公開鍵暗号方式において、前記前バージョン扱い識別子Ｆは、前記複合鍵の変更の遡及的適用の有無を識別する情報を含むことを特徴とする。

【００２２】また、本発明の公開鍵暗号方式は、少なくとも平文を共通鍵Ｋにより暗号化した暗号情報Ｋ（Ｄ）と、１以上のメンバＭｉ（ｉ＝１～ｎ）を構成員とするグループに属するメンバ個々の公開鍵Ｐｉによって前記共通鍵Ｋを暗号化した１以上のＰｉ（Ｋ）とを有する構成データを暗号情報として構成したことを特徴とする。

【００２３】また、本発明の暗号化装置は、平文を暗号化するデータ変換のために用いられる第１の鍵と、該第１の鍵と異なる鍵であり、暗号を復号し平文とするデータ変換のために用いられる第２の鍵との組み合わせによって構成される公開鍵暗号方式における暗号化装置において、１以上のメンバＭｉ（ｉ＝１～ｎ）を構成員とするグループを単位として割り当てられるグループ公開鍵P_Gを用いて平文をデータ変換することにより、暗号化する暗号化手段と、前記メンバＭｉの公開鍵P_{Mi}によって前記グループを単位として割り当てられるグループ秘密鍵S_Gをデータ変換し暗号化することにより、１以上の暗号化グループ秘密鍵P_{Mi}（S_G）（ｉ＝１～ｎ）を生成する暗号化秘密鍵生成手段と、を有することを特徴とする。

【００２４】また、本発明の暗号化装置は、グループ単位毎に公開鍵と秘密鍵とを生成する鍵生成手段を有し、該鍵生成手段が生成した公開鍵および秘密鍵を前記グループ公開鍵P_Gとグループ秘密鍵S_Gとして割り当てることを特徴とする。

【００２５】また、本発明の暗号化装置は、前記グループ公開鍵P_Gにより暗号化された前記暗号情報に対して、該暗号化を実行するメンバまたは該メンバが属するグループの秘密鍵を適用して署名した電子署名ブロックと該適用した秘密鍵の公開鍵とを含む署名情報を生成することを特徴とする。

【００２６】また、本発明の暗号化装置は、自己の使用可能なグループ公開鍵または個人公開鍵の少なくともいずれか一方を含む公開鍵リストを有し、該公開鍵リストから選択した暗号の復号を可能とするメンバＭｉの公開鍵P_{Mi}を用いて前記グループ秘密鍵S_Gのデータ変換による１以上の暗号化グループ秘密鍵P_{Mi}（S_G）（ｉ＝１～ｎ）を生成することを特徴とする。

【００２７】また、本発明の暗号化装置は、１以上のメンバＮｊ（ｊ＝１～ｍ）を構成員とするグループを単位として生成されるグループ公開鍵P_Cおよびグループ秘密鍵S_Cと、前記メンバＮｊに固有の公開鍵P_{Nj}の各々によって前記グループ秘密鍵S_Cのデータ変換を実施して暗号化された１以上の暗号化グループ秘密鍵P_{Nj}（S_C）（ｊ＝１～ｍ）とを構成要素として有する複合鍵のグループ公開鍵P_Cを前記公開鍵リストが含む場合において前記複合鍵の変更に応じて前記公開鍵リストを更新する手段を有することを特徴とする。

【００２８】また、本発明の復号装置は、平文を暗号化するデータ変換のために用いられる第１の鍵と、該第１の鍵と異なる鍵であり暗号を復号し平文とするデータ変換のために用いられる第２の鍵との組み合わせによって構成される公開鍵暗号方式における復号装置において、暗号文の復号に用いる復号鍵Ｓを暗号の受け手の公開鍵Ｐｊで暗号化した暗号化秘密鍵Ｐｊ（Ｓ）を自己またはグループの秘密鍵Ｓｊにより復号する秘密鍵復号手段と、前記秘密鍵復号手段により復号し、獲得した復号鍵Ｓにより、前記暗号文を復号する復号手段と、を備えたことを特徴とする。

【００２９】また、本発明の復号装置は、前記暗号化された暗号情報が、他の暗号情報の復号鍵Ｓ１であり、前記復号手段により獲得した前記復号鍵Ｓ１によって前記他の暗号情報の復号を実行する手段を有することを特徴とする。

【００３０】また、本発明の復号装置は、１以上のメンバＮｊ（ｊ＝１～ｍ）を構成員とするグループを単位として生成されるグループ公開鍵P_Cおよびグループ秘密鍵S_Cと、前記メンバＮｊに固有の公開鍵P_{Nj}の各々によって前記グループ秘密鍵S_Cのデータ変換を実施して暗号化された１以上の暗号化グループ秘密鍵P_{Nj}（S_C）（ｊ＝１～ｍ）とを構成要素として有する複合鍵の前記暗号化グループ秘密鍵P_{Nj}（S_C）（ｊ＝１～ｍ）から自己の秘密鍵S_{Nj}により前記グループ秘密鍵S_Cを復号し、前記秘密鍵復号手段は該復号したグループ秘密鍵S_Cを用いて前記復号鍵Ｓを獲得することを特徴とする。

【００３１】また、本発明の復号装置は、前記秘密鍵復号手段によって復号したグループ秘密鍵S_{C1}を用いて他の複合鍵における暗号化グループ秘密鍵からグループ秘密鍵S_{C2}を復号する操作を再帰的に行う再帰的実行手段と、前記再帰的実行手段により復号したグループ秘密鍵を適用することにより、暗号化された「暗号情報の復号鍵」を復号する手段を有することを特徴とする。

【００３２】また、本発明の復号装置は、暗号文を復号するデータ変換の際に使用する秘密鍵リストを有し、該秘密鍵リストは、自己の秘密鍵を用いて復号することに

より獲得可能な複合錠を登録したリストであることを特徴とする。

【００３３】また、本発明の復号装置は、前記秘密錠リスト中に含まれる複合錠には、自己の秘密鍵により直接的に復号鍵を得ることが可能な個人錠と、自己の秘密鍵の適用により暗号化秘密鍵を復号し、間接的に復号鍵を得ることが可能なグループ錠とが区分されていることを特徴とする。

【００３４】また、本発明の復号装置は、新たに取得した複合錠が有するバージョン扱い識別子Ｆに基づいて、前記秘密錠リストの内容を更新する手段を有することを特徴とする。

【００３５】また、本発明の暗号化方法は、平文を暗号化するデータ変換のために用いられる第１の鍵と、該第１の鍵と異なる鍵であり、暗号を復号し平文とするデータ変換のために用いられる第２の鍵との組み合わせによって構成される公開鍵暗号方式における暗号化方法において、１以上のメンバＭｉ（ｉ＝１～ｎ）を構成員とするグループを単位として生成されるグループ公開鍵P_Gを用いて平文をデータ変換することにより、暗号化するステップと、前記メンバＭｉの公開鍵P_{Mi}によって前記グループを単位として生成されるグループ秘密鍵S_Gをデータ変換し暗号化することにより、１以上の暗号化グループ秘密鍵P_{Mi}（S_G）（ｉ＝１～ｎ）を生成するステップと、を有することを特徴とする。

【００３６】また、本発明の復号方法は、平文を暗号化するデータ変換のために用いられる第１の鍵と、該第１の鍵と異なり、暗号を復号し平文とするデータ変換のために用いられる第２の鍵との組み合わせによって構成される公開鍵暗号方式における復号方法において、１以上のメンバＭｉ（ｉ＝１～ｎ）を構成員とするグループを単位として生成されるグループ秘密鍵S_Gの前記メンバの公開鍵P_{Mi}による暗号化により生成された暗号化グループ秘密鍵P_{Mi}（S_G）を前記メンバの秘密鍵S_{Mi}によって復号し、前記グループ秘密鍵S_Gを獲得するステップと、前記グループを単位として生成されるグループ公開鍵P_Gにより暗号化された情報を、前記獲得されたグループ秘密鍵S_Gを用いてデータ変換することにより暗号化情報を復号するステップと、を有することを特徴とする。

【００３７】また、本発明の複合錠生成方法は、平文を暗号化するデータ変換のために用いられる第１の鍵と、該第１の鍵と異なり、暗号を復号し平文とするデータ変換のために用いられる第２の鍵との組み合わせによって構成される公開鍵暗号方式であり、１以上のメンバＭｉ（ｉ＝１～ｎ）を構成員とするグループを単位として生成されるグループ公開鍵P_Gおよびグループ秘密鍵S_Gと、前記メンバＭｉに固有の公開鍵P_{Mi}の各々によって、前記グループ秘密鍵S_Gのデータ変換を実行し暗号化された１以上の暗号化グループ秘密鍵P_{Mi}（S_G）（ｉ＝１～ｎ）とを構成要素として有する複合錠を使用する公開鍵暗号方式における複合錠の生成方法であって、１以上のメンバＭｉ（ｉ＝１～ｎ）を構成員とするグループを単位として公開鍵P_Gと秘密鍵S_Gとを生成するステップと、前記メンバＭｉに固有の公開鍵P_{Mi}の各々によって、前記生成されたグループ秘密鍵S_Gのデータ変換を実行し暗号化された１以上の暗号化グループ秘密鍵P_{Mi}（S_G）（ｉ＝１～ｎ）を生成するステップと、複合錠の変更を制御する複合錠変更秘密鍵S_Uを、変更を行う権利を有するメンバ固有の公開鍵P_{Ui}によるデータ変換によって暗号化された１以上の暗号化複合錠変更秘密鍵P_{Ui}（S_U）を生成するステップと、前記生成された公開鍵P_G、暗号化グループ秘密鍵P_{Mi}（S_G）および暗号化複合錠変更秘密鍵P_{Ui}（S_U）とを含むデータに対して前記生成された複合錠変更秘密鍵S_Uを用いて電子署名を行うステップと、を有することを特徴とする。

【００３８】また、本発明の複合錠変更方法は、平文を暗号化するデータ変換のために用いられる第１の鍵と、該第１の鍵と異なり、暗号を復号し平文とするデータ変換のために用いられる第２の鍵との組み合わせによって構成される公開鍵暗号方式であり、１以上のメンバＭｉ（ｉ＝１～ｎ）を構成員とするグループを単位として生成されるグループ公開鍵P_Gおよびグループ秘密鍵S_Gと、前記メンバＭｉに固有の公開鍵P_{Mi}の各々によって、前記グループ秘密鍵S_Gのデータ変換を実行し暗号化された１以上の暗号化グループ秘密鍵P_{Mi}（S_G）（ｉ＝１～ｎ）と、複合錠の変更を制御する複合錠変更秘密鍵S_Uを、変更を行う権利を有するメンバ固有の公開鍵P_{Ui}によるデータ変換によって暗号化された１以上の暗号化複合錠変更秘密鍵P_{Ui}（S_U）とを構成要素として有する複合錠を使用する暗号化方式における複合錠の変更方法であって、複合錠の内容を変更するステップと、前記暗号化複合錠変更秘密鍵P_{Ui}（S_U）から自己の秘密鍵S_{Ui}を用いて復号することにより複合錠変更秘密鍵S_Uを得るステップと、前記公開鍵P_G、暗号化グループ秘密鍵P_{Mi}（S_G）および暗号化複合錠変更秘密鍵P_{Ui}（S_U）とを含むデータに対して前記生成された複合錠変更秘密鍵S_Uを用いて電子署名を行うステップと、を有することを特徴とする。

【００３９】また、本発明の複合錠変更方法は、複合錠の変更を制御する複合錠変更公開鍵P_Uおよび複合錠変更秘密鍵S_Uの新たなペアを生成するステップと、前記複合錠の変更を行う権利を有するメンバ固有の公開鍵P_{Ui}によるデータ変換によって暗号化した１以上の暗号化複合錠変更秘密鍵P_{Ui}（S_U）を生成し、複合錠に付与するステップと、を有することを特徴とする。

【００４０】また、本発明の複合錠変更方法は、変更された複合錠を構成するデータに対し前記複合錠変更秘密鍵S_Uにより電子署名した結果である署名ブロックを前

記変更された複合鍵を構成するデータに新たに付与し、該署名ブロックを含めた全体を新たな複合鍵とし、該新たな複合鍵に対して前記複合鍵変更前の変更用秘密鍵S_Uで署名するステップを有することを特徴とする。

【００４１】また、本発明の複合鍵変更方法は、平文を暗号化するデータ変換のために用いられる第１の鍵と、該第１の鍵と異なり、暗号を復号し平文とするデータ変換のために用いられる第２の鍵との組み合わせによって構成される公開鍵暗号方式であり、１以上のメンバＭｉ（ｉ＝１～ｎ）を構成員とするグループを単位として生成されるグループ公開鍵P_Gおよびグループ秘密鍵S_Gと、前記メンバＭｉに固有の公開鍵P_{Mi}の各々によって、前記グループ秘密鍵S_Gのデータ変換を実行して暗号化された１以上の暗号化グループ秘密鍵$P_{Mi}(S_G)$（ｉ＝１～ｎ）とを構成要素として有する複合鍵を使用する公開鍵暗号方式における複合鍵変更方法において、メンバの変更が現時点以降の変更である場合は、新たなグループ公開鍵P_Gと新たなグループ秘密鍵S_Gとのペアを生成し、該複合鍵の新たな公開鍵および秘密鍵として用い、メンバの変更が過去に遡る変更の場合には、現在のグループ公開鍵P_Gとグループ秘密鍵S_Gとのペアをそのまま継続して該複合鍵の公開鍵および秘密鍵として用いることを特徴とする。

【００４２】また、本発明の公開鍵暗号方式における暗号化方法を記録したコンピュータ読み取り可能な記録媒体は、平文を暗号化するデータ変換のために用いられる第１の鍵と、該第１の鍵と異なる鍵であり、暗号を復号し平文とするデータ変換のために用いられる第２の鍵との組み合わせによって構成される公開鍵暗号方式における暗号化方法を記録したコンピュータ読み取り可能な記録媒体において、１以上のメンバＭｉ（ｉ＝１～ｎ）を構成員とするグループを単位として生成されるグループ公開鍵P_Gを用いて平文をデータ変換することにより、暗号化するステップと、前記メンバＭｉの公開鍵P_{Mi}によって前記グループを単位として生成されるグループ秘密鍵S_Gをデータ変換し暗号化することにより、１以上の暗号化グループ秘密鍵$P_{Mi}(S_G)$（ｉ＝１～ｎ）を生成するステップと、を実行するプログラムを記録したことを特徴とする。

【００４３】また、本発明の公開鍵暗号方式における復号方法を記録したコンピュータ読み取り可能な記録媒体は、平文を暗号化するデータ変換のために用いられる第１の鍵と、該第１の鍵と異なり、暗号を復号し平文とするデータ変換のために用いられる第２の鍵との組み合わせによって構成される公開鍵暗号方式における復号方法を記録したコンピュータ読み取り可能な記録媒体において、１以上のメンバＭｉ（ｉ＝１～ｎ）を構成員とするグループを単位として生成されるグループ秘密鍵S_Gの前記メンバの公開鍵P_{Mi}による暗号化により生成された暗号化グループ秘密鍵$P_{Mi}(S_G)$を前記メンバの秘密鍵S_{Mi}によって復号し、前記グループ秘密鍵S_Gを獲得するステップと、前記グループを単位として生成されるグループ公開鍵P_Gにより暗号化された情報を、前記獲得されたグループ秘密鍵S_Gを用いてデータ変換することにより暗号化情報を復号するステップと、を実行するプログラムを記録したことを特徴とする。

【００４４】

【発明の実施の形態】本発明の概要をまず述べる。以下の説明において個人の集合をグループと呼び、グループの要素、すなわち構成員である個人をメンバと呼ぶ。本発明は、公開鍵暗号方式において、グループの概念を導入したものである。すなわち、特定のグループに属する任意のメンバが復号可能である暗号化と、特定のグループに属する任意のメンバによる署名を代表的な機能とする暗号方式である。本発明では、グループ秘密鍵による署名を可能とすることにより、実際に署名したメンバを明確にせずグループ内のメンバによる署名であることのみを明らかにできるという利点を有する。

【００４５】グループに対応する秘密鍵と公開鍵のペアを提供し、それぞれをグループ秘密鍵、グループ公開鍵と呼ぶ。グループ秘密鍵をすべてのメンバの個人公開鍵でそれぞれ暗号化し、その暗号化されたグループ秘密鍵の集合を作り、この暗号化されたグループ秘密鍵の集合は、少なくとも各メンバが入手可能なものとしておく。これにより、グループ内の任意のメンバは、自分自身の個人秘密鍵を用いて、対応する個人公開鍵で暗号化されたグループ秘密鍵を復号すること、すなわち獲得することができる。よって、グループ公開鍵で任意の情報を暗号化すれば、グループのメンバは、その暗号化された情報を上記の手法で獲得したグループ秘密鍵を使用して復号することができる。同様に、グループのメンバは、グループ秘密鍵を使用して署名を行うことができる。

【００４６】本発明は、これらの機能を実現するために必要となるグループ秘密鍵およびグループ公開鍵のペアの生成、グループ公開鍵による暗号化処理、グループ秘密鍵による復号処理、さらにグループのメンバの追加、削除等の変更の際の処理について明らかにする。

【００４７】情報の暗号化により、情報の機密性を保持しようとする場合には、暗号化された情報自体の所在は問わない、すなわち明らかにされない。このことは、一旦、暗号化された情報を、何らかの理由により、暗号化し直さなければならない機構は受け入れがたいことを意味する。なぜなら、所在を問わないということは、暗号化し直さなければならない情報の所在の特定が困難であるからである。そのため、本発明ではグループの構成員であるメンバに変更があった場合は、一旦、暗号化された情報の再暗号化ではなく、鍵の作り直しで対応することになる。従来の個人を単位とする公開鍵暗号方式では、恒久的な存在である個人と鍵が１体１対応であり、鍵の作り直しという要請はなかったが、本発明では、グ

ループ対鍵という対応関係が発生し、グループの構成要素の変更に基づく鍵の変更要請が発生する。

【００４８】本発明の暗号および署名方式は、上述のグループ単位の暗号化および署名のみではなく、組織内の特定の役割を果たすポジションにある個人、例えば企業内の人事部長といった役割に対応する鍵を提供する場合にも有効な機能を持つ。例えば、人事部長の役割に対応する鍵があり、人事部長を努める個人が変更された場合には、人事部長という役割に対応する鍵を変更することによって実世界の変更に対応可能である。人事部長に対して暗号化文書を送付する側は、従来からの当該役割（人事部長）に対応する公開鍵を使用して情報を暗号化すればよい。また、新たな人事部長は、すでに暗号化されている情報を変更することなく、過去に当該役割に対応する公開鍵を使用して暗号化された情報を参照することが可能となる。

【００４９】企業内のプロジェクト等ある目的を有するグループにおいては、複数人による協同作業や役割に基づいた作業が重要であり、その協同作業グループのメンバや、役割を果たす個人は固定的なものではない。従って、グループの中と外との機密性保持能力はより高度なものが要求される。

【００５０】また、情報ネットワークサービスにおいて公証局と呼ばれる公開鍵に対する所定レベルの保証を与えるシステムが利用されつつあるが、本発明においては、公証局を利用することによって無効となった鍵の排除が可能である。

【００５１】次に、本発明を構成する各要素について説明する。説明は以下の項目について行う。

（１）複合錠
（２）グループ錠
（３）個人錠
（４）個人錠の秘密鍵
（５）複合錠リスト
（６）信用体
（７）公証局

【００５２】（１）複合錠

複合錠は、次に説明するグループ錠（役割錠）、個人錠を実現する錠の総称であり、具体的には以下の要素を持つ電子データである。

【００５３】ａ．名前

複合錠に対応する実世界の実態を意味する人間が可読な文字列であり、複合錠の識別子としての役割を有する。人間が異なる文字列を同一と誤って判断することを防ぐためスペースあるいは混同されやすい文字列の使用はしないことが好ましい。

【００５４】ｂ．作成日時、作成者

複合錠を作成した日時、および複合錠の作成者である。作成者は、作成した複合錠全体に対する署名を行う。署名の手順には、複合錠を構成する電子データを作成者の個人鍵で暗号化することが含まれる。

【００５５】ｃ．秘密鍵のリスト

複合錠の秘密鍵を、メンバの公開鍵で暗号化し、メンバの名前（メンバを識別するデータであればよい）をラベルとして付与したもののリストである。メンバの秘密鍵によって復号することにより、複合錠の秘密鍵を獲得できる。複合錠の秘密鍵を用いて他から送付された暗号の復号が可能である。

【００５６】ｄ．公開鍵

複合錠の公開鍵である。情報を暗号化する際には、この公開鍵によってデータ変換を実行し、暗号とする。

【００５７】ｅ．変更錠の秘密錠リスト

情報の機密性保持等に用いる公開鍵と秘密鍵のペアとは独立に、複合錠の変更権を制御するための公開鍵と秘密鍵とのペアが必要となる。このペアを変更錠と呼ぶ。この変更錠の秘密鍵を、変更権所有者の公開鍵で暗号化し、変更権所有者の名前をラベルとして付与したもののリストを複合錠は保持する。複合錠の変更権所有者のみが、その複合錠の変更、例えば、メンバの追加、削除等を行い新しいバージョンの複合錠を作成することが許される。この変更権所有者は予め指定される。ある複合錠が変更権所有者によって変更され、新しいバージョンとなったときは、旧バージョンの錠を信用している人は、新バージョンの錠を自動的に信用するように設定できる。これを自動信用機構と呼ぶ。錠の信用については後述する。正当な変更権所有者によって複合錠の変更が行われたことを明確にするために、変更に際しては、変更錠の秘密鍵による署名を行う。ただし、複合錠のメンバ全員がその複合錠の変更権を有する場合には、機密保持用のペアを用いる。この場合には、現バージョンの秘密鍵による署名を行う。

【００５８】ｆ．変更錠の公開鍵

上述の変更錠の秘密鍵とペアを構成するものであり、上記の変更錠の秘密鍵による署名された複合錠の復号等に使用され、署名の確認が可能となる。なお、以上に加えて複合錠の有効期限や公証局と交信できないオフライン期間における有効期間を付加し、複合錠の利用を制御するようにしてもよい。

【００５９】（２）グループ錠

グループ錠とは、実世界のグループに対応する複合錠である。グループは一般に複数のメンバを含む。役割錠（例えば人事部長の役割）としても機能する。

【００６０】（３）個人錠

個人錠は、個人に対応する複合錠である。個人錠も複合錠により実現される。個人錠としての複合錠のメンバは、供託者を指定する。供託者とは、その個人以外の人に対して条件付きでその個人と同一の権利が与えられた人のことである。これは、その個人がパスフレーズを忘れた場合等、その個人の代理者としての役割を果たしうる人を供託者として情報の復号を可能とする。これは、

例えば企業内での情報の機密性、および復号可能性を１人の個人に託する危険性を考慮したものである。また、情報の監査や検閲を行うために用いることも可能である。供託者が個人錠を利用することができる条件として複数の指定された供託者の承認を必要とするといった設定も可能である

【００６１】（４）個人錠の秘密鍵

個人錠の秘密鍵はパスフレーズと呼ばれる利用者のみが知っている文字列をキーとして暗号化された形でのみ存在する。個人錠の秘密鍵が必要になった時点で、パスフレーズが入力され、個人錠の秘密鍵が直接入手できる。

【００６２】（５）複合錠リスト

個人が所有する信用度が明確な複合錠リストである。複合錠とその対応する信用度がペアとして保持される。複合錠を利用するときは、このリスト中の信用度により判断される。ここに存在しない複合錠の信用度は不明であると解釈される。例えば、暗号文の復号を許容する個人またはグループをこの複合錠リストで指定し、対応する複合錠からその公開鍵を取得して暗号化秘密鍵を生成する際に用いられる。すなわち、この複合錠のリストは信用した個人やグループの公開鍵を間接的に登録した公開錠リストであり、個人やグループの公開鍵を直接登録するものであってよい。なお、複合錠そのものは、装置に記憶されたもの以外に、遠隔に位置する装置に記憶されたものを参照するものでもよく、装置内および装置外に記憶された複合錠を混在して用いるものであってもよい。

【００６３】（６）信用体

本発明におけるグループにおいて使用される複合錠は、誰でも生成できるが、信用されないと有効な錠とは成り得ない。複合錠を信用するとは、実世界の実態として存在するグループ（役割を含む）と、そのグループに対応するであろう複合錠とが実際に対応することを信用するという意味である。具体的には、単にグループと複合錠とが対応するだけではなく、信用する時点での実世界のグループのメンバと複合錠に含まれるメンバとが一致しなければならない。例えば「人事部人事１課」という名称の複合錠があったとする。「人事部人事課」という実世界のグループは存在するが、「人事部人事１課」という実世界のグループは存在しないかもしれない。「人事部人事１課」という実世界のグループが存在したとしても、それに対応する正当な複合錠は存在していないかもしれない。よって複合錠の名称のみを根拠に複合錠を信用することはできない。また、「人事部人事１課」内のメンバが変更されたにもかかわらず複合錠のメンバ中に過去のメンバが残っているような場合には信用することができない。

【００６４】どの複合錠が信用できるかについての情報を信用情報という。また、信用情報自体の信用度を示す情報も信用情報である。信用情報を保持する主体を信用体という。信用情報、および複合錠を何を根拠として信用するのかは信用体の任意である。信用体には、個人と以下の（７）で説明する公証局の２種類が存在する。信用体は他の信用体を信用することができる。このとき信用される信用体を被信用体と呼ぶ。信用体は、複合錠を信用しているときにのみ、この複合錠を利用することになる。信用体がその複合錠に対する直接の信用情報を持たない場合は、信用している信用体がその複合錠を信用している場合には信用する。とすることが可能である。

【００６５】例えば、個人「田中さん」および公証局「Ｘ商事」がいずれも信用体であるとき、個人「田中さん」が公証局「Ｘ商事」を信用しているとき、公証局「Ｘ商事」が信用しているものは、個人「田中さん」は自動的に信用する。しかし、逆に個人「田中さん」が信用しているものを公証局「Ｘ商事」が信用するとは限らない。という関係である。

【００６６】信用の程度には種類があり、信用レベルと呼ばれる。この信用レベルを使用して信用度の未知の複合錠の信用度を演算によって求めることが可能である。このとき使用される信用レベルは、例えば以下の表の信用レベルである。

【００６７】

【表１】

レベル◎：完全に信用する（ｅｘ．自分自身）。

レベル○：十分に信用する。

レベル△：ある程度信用する。

レベル？：不明。

レベル×：信用しない。

【００６８】信用レベルが未知の複合錠に対する信用レベルを同一の複合錠に対する独立した異なる２つの信用体、例えば２人の個人Ａ、Ｂの有するその複合錠に対する信用レベルから求める場合の例を図１に示す。図１の第１行は個人Ａ、左端列は個人Ｂの信用レベルを示すもので、それぞれの場合についての結果が表として示されている。例えば個人Ａの設定した信用レベルが○であり、Ｂが設定した信用レベルが？である複合錠の信用レベルは○となる。

【００６９】また、信用体に対する信用レベルと、その信用体の他の信用体への信用レベルまたは複合錠への信用レベルを使用した信用レベルの演算には、例えば図２に示すような演算規則が使用される。図２の第１行は信用体に対する信用レベル、左端列はその信用体の他の信用体への信用レベルまたは複合錠への信用レベルを示すもので、それぞれの場合についての結果が表として示されている。例えばその信用体の信用レベルが○であり、その信用体が設定した信用レベルが？である複合錠の信用レベルは？となる。このような図１あるいは図２で示す演算規則を用いて信用度が未知の信用体あるいは複合錠の信用度を決定することが可能である。

【００７０】（７）公証局

公証局は、上述のように信用体の１つである。公証局の提供する機能は、例えばある暗号システムが使用されている企業や組織といった単位での公の信用を表現、提供することである。公証局における複合錠の信用基準は、当該公証局を運営する企業や組織が任意に決定する。この信用基準の決定方式には、次に述べるようないくつかの方式が考えられる。以下の説明において「保証する」とは、登録されようとする複合錠が正当であることを登録者以外の個人が証明する行為をいう。

【００７１】ａ）公証局の特定の管理者による何らかの手続により正当であることを確認する。確認がなされた場合に、公証局がその複合錠を信用する。ここで何らかの手続とは、実世界における任意の手続である。例えば申請用紙に捺印がおされていること、あるいは、申請者の身分証明書の確認手続による等である。この他、名前の重複確認、登録者毎に指定されている他の特定の個人による保証、予め決められた人数以上の保証、または、公証局の信用している個人の署名が予め決められた人数以上の場合等に信用して登録するようにしてもよい。

【００７２】

【実施例】以下、グループ錠を用いた暗号方式の実施例を示す。なお、ここでは、上述の説明における複合錠の中のグループ錠を取り上げて説明するが、複合錠のもう１つの種類である個人錠においても、グループ錠におけるメンバが供託者に変更になる他は、同様の構成、手続で暗号方式が構成される。また、グループ錠の特殊な用途として上述した役割錠があるが、グループ錠を役割錠として機能させるためには、グループ錠の構成メンバ数を１とし、その唯一のメンバとして、現在その役割を果たしている個人とすればよい。ただし、副社長の役割錠のメンバに副社長自身の他にその秘書を含めるといった運用も可能である。

【００７３】本発明の暗号方式を利用する各人は２つの錠リストを有する。すなわち、ａ）各人が信用しているグループ錠および個人錠のリストである「公開錠リスト」、および、ｂ）各人が自身の秘密鍵を元に直接もしくは間接に秘密鍵を獲得できるグループ錠のリストである「秘密錠リスト」である。ここでは、簡単のために、「公開錠リスト」に含まれているグループおよび個人錠は信用しているものとし、「やや信用している」といった中程度の信用を与えることはしない。また、信用するか否かは、上述の信用程度の演算規則を用いたものあるいは利用者の判断等に基づくものとし、以下の実施例中での詳細な説明は省略する。ただし、グループ錠を変更した際に、直前のグループ錠を信用している場合における自動信用機構、すなわち変更前のグループ錠を信用している場合は、変更後のグループ錠を自動的に信用するものとする。また、上述の公証局への登録手続についても以下の実施例中では直接触れないが、上述した説明のようにネットワーク中に公証局がある場合には、生成、あるいは変更された錠については、公証局への登録がなされる。ただし、この登録手続は、本発明の必須要件ではない。

【００７４】まず、この実施例の全体構成を図３により説明する。本実施例の基本的な機能は、個人対個人で、情報を正確に機密性を保持して伝達することである。ただし、個人は、グループに所属していることもある。情報の伝達は、メールのような直接伝送する方法でも、ファイルサービスを介した間接的な方法でも良い。

【００７５】図３に示すように個人間で伝達するものは、暗号だけでなく、必要に応じて個人公開鍵や、グループ錠も伝達する。個人公開鍵やグループ錠はともに、それが実世界に実在する個人やグループとの正しい対応関係にあるか否かの判断を必要とする場合には、その判断手続を確立することが必要となる。

【００７６】図３に示す「個人」における平文から暗号への暗号化の際には、復号可能とすべき個人やグループを自身が保持する錠に対応する錠を錠リストから選択して、暗号化する。これにより、選択した個人や、選択したグループに属する個人が復号可能な暗号が生成される。または、共通鍵ＫＡによって平文を暗号化するとともに、この暗号の復号に必要な復号鍵ＫＢを復号可能とすべき個人やグループを自身が保持する錠に対応する錠を錠リストから選択して、暗号化し、これらを送付する。

【００７７】伝達された暗号化情報を復号する際には、得られた暗号が自身の個人秘密鍵によって直接復号可能であれば、自身の個人秘密鍵を用いて復号する。自身が間接もしくは直接に属するグループによって復号可能であれば、自身の個人秘密鍵を用いてグループ錠をグループ秘密鍵に変換することでグループ秘密鍵を獲得し、それを用いて復号する。グループ秘密鍵は利用後直ちに捨て、単独では保持しない。本方式において、「個人」に秘密遵守を要請されるのは、個人秘密鍵だけである。共通鍵ＫＡによって暗号化が実行された場合には、まず、復号に必要な復号鍵ＫＢを自身の個人秘密鍵を用いて復号する。自身が間接もしくは直接に属するグループによって復号可能であれば、自身の個人秘密鍵を用いてグループ錠をグループ秘密鍵に変換することでグループ秘密鍵を獲得し、それを用いて復号鍵ＫＢを獲得し、この復号鍵ＫＢによって平文を復号する。

【００７８】［グループ錠］本実施例におけるグループ錠の構造を図４に示す。図４における各記号の説明を次に示す。

【００７９】L_G：このグループ錠のラベル
文字列である。ある個人の錠リストの中では重複を許さない。全体としては重複は生じうるので、識別子として利用することはしない。ただし、ラベルが一致しなければ公開鍵も一致しないため、そのことを利用して処理を高速化することはできる。

【００８０】P_G：このグループ錠の公開鍵
利用する公開鍵暗号システムに応じた公開鍵であり、一般に５１２ビットから２０４８ビット程度の固定長のデータ列である。このグループに直接もしくは間接に属するすべての個人に復号可能な暗号化を行う際には、この公開鍵を用いて暗号化する。また、このグループに直接もしくは間接に属する任意の個人として署名されたものを確認する際には、この公開鍵を用いて署名の確認を行う。公開鍵はグループ錠の中に、そのままの形式で含まれており、誰でもが参照できる。
【００８１】S_G：このグループ錠の秘密鍵
利用する公開鍵暗号システムに応じた秘密鍵であり、一般に５１２ビットから２０４８ビット程度の固定長のデータ列である。対応する公開鍵で暗号化された暗号を復号する際に用いる。また、このグループに直接もしくは間接に属する任意の個人として署名する際にも用いる。この秘密鍵は、直接もしくは間接的に個人の秘密鍵により暗号化されており、利用する際には、個人の秘密鍵を用いて逐次復号して獲得し、利用後はすぐに捨て去り、単独で保持することはしない。
【００８２】Ｍｉ：このグループのメンバ
概念上の存在であり、データ構造には直接現れない。メンバには個人およびグループがなり得る。なお、前述のようにグループ錠ではなく個人錠の場合には、このメンバは供託者となる。
【００８３】P_U：このグループ錠変更用の公開鍵
利用する公開鍵暗号システムに応じた公開鍵であり、一般に５１２ビットから２０４８ビット程度の固定長のデータ列である。グループはメンバの追加もしくは削除といった変更を行う必要がある。その変更を行える権利を持つ人を識別する方法として、専用の公開鍵と秘密鍵の対を利用する。これはその公開鍵である。グループ錠には、変更用の秘密鍵が、変更権を所有する個人の個人秘密鍵により直接もしくは間接に暗号化されて含まれている。グループ錠を変更したときには、新しいグループ錠をその変更用秘密鍵により署名する。変更用秘密鍵は変更権の所有者でなければ入手できないため、その署名が確認できれば正当な変更権の所有者による変更であることが確認できる。この確認処理は、以前のグループ錠を信用していれば自動的に行うことができる。この変更用公開鍵は、そのままの形式で含まれているため誰でも参照できる。
【００８４】S_U：このグループ錠変更用の秘密鍵
利用する公開鍵暗号システムに応じた秘密鍵であり、一般に５１２ビットから２０４８ビット程度の固定長のデータ列である。機能は、P_Uの説明に記載のとおりである。
【００８５】Ｖ：このグループ錠のバージョン番号
自然数である。新規にグループ錠を生成したときには、１となる。グループ錠のバージョンを示す。変更するとバージョン番号は基準となったバージョンより１多い数とする。
【００８６】Ｆ：直前のバージョンの扱いを示す値
「不要」、「必要」、「抹消」のいずれかの値を取る。グループ錠の変更を行った際、直前のバージョンを持つ個人は、新しいバージョンを入手することにより直前のバージョンを適切に扱う必要がある。「不要」は、直前のバージョンが不要となることを意味する。「必要」は、直前のバージョンにより作られた暗号を復号するため、直前のバージョンによりなされた署名を確認するために必要である。この場合には、新たに暗号化や署名を行うときには最新のバージョンを使わなければならない。「抹消」は、「必要」に近いが、自身が新しいバージョンの秘密鍵を獲得できない場合には、直前のバージョンを削除しなければならないことを意味する。新規にグループ錠を生成したときには、この値は意味を持たない。
【００８７】Ｕｉこのグループの変更権所有者
概念上の存在であり、データ構造には直接現れない。変更権所有者には、個人およびグループを指定できる。
【００８８】L_{Mi}：Ｍｉのラベル
文字列である。このグループ錠の直接のメンバである、他のグループ錠もしくは個人公開鍵のラベルである。個人錠については、本実施例においては明記しないが、対応する個人が管理する秘密鍵と、公開する公開鍵とからなり、少なくとも公開鍵にはラベルが付与されているとする。
【００８９】P_{Mi}：Ｍｉの公開鍵
利用する公開鍵暗号システムに応じた公開鍵であり、一般に５１２ビットから２０４８ビット程度の固定長のデータ列である。このグループの直接のメンバの公開鍵である。
【００９０】P_{Mi}（S_G）：P_{Mi}で暗号化されたS_G
利用する公開鍵暗号システムに応じた暗号処理により、S_Gを暗号化した結果である。これを用いてS_Gを獲得するためには、P_{Mi}に対応する秘密鍵S_{Mi}が必要である。これは、対応するL_{Mi}をインデックスとした配列により保持する。
【００９１】L_{Ui}：Ｕｉのラベル
文字列である。このグループ錠の変更権所有者である個人の個人錠のラベルである。
【００９２】P_{Ui}：Ｕｉの公開鍵
利用する公開鍵暗号システムに応じた公開鍵であり、一般に５１２ビットから２０４８ビット程度の固定長のデータ列である。このグループ錠の変更権所有者である個人の公開鍵もしくはグループ錠の公開鍵である。
【００９３】P_{Ui}（S_{Ui}）：Ｕｉの公開鍵で暗号化されたS_U
利用する公開鍵暗号システムに応じた暗号処理により、S_Gを暗号化した結果である。これを用いてS_Gを獲得す

るためには、P_{Ui}に対応する秘密鍵S_{Ui}が必要である。これは、対応するL_{Ui}をインデックスとした配列により保持する。なお、本実施例では、パケット通信におけるパケットのデータ構造のように、秘密鍵に対してデータを識別するための情報を付加した上で暗号化を行う。従って、この暗号化秘密鍵を復号した際に付加的情報に基づいて秘密鍵が正常に復号されたか否かを容易に判別することができる。

【００９４】Ｓｉｇ（S_U）：全体に対するS_Uによる署名

署名を示すデータ列である。ここで全体とは、L_G、P_G、Ｖ、Ｆ、P_U、L_{Mi}、P_{Mi}（S_G）、L_{Ui}、P_{Ui}（S_U）である。署名とは、秘密鍵S_Uによる暗号化処理である。公開鍵暗号システムでは、通常と逆に、秘密鍵により暗号化し、それを公開鍵で復号することができる。公開鍵で復号できるには、秘密鍵により暗号化しなければならないため、公開鍵で復号できることを確認することにより、秘密鍵により署名されたことを確認できる。実際には、メッセージダイジェストをその対象範囲に対して行い、その処理結果に対して、秘密鍵S_Uにより署名する。メッセージダイジェストとは、署名の対象範囲を全て暗号化するにはコストがかかるために、対象範囲のデータサイズには独立に、対象範囲の内容に応じて１２８ビット程度の情報を生成する処理である。メッセージダイジェスト処理アルゴリズムは公開されたものを用い、鍵も利用しない。よって確認の際には、対象データをメッセージダイジェストし、署名を復号した結果と一致するか否かを確認することになる。メッセージダイジェストの処理は、チェックサムに類似した処理であるが、処理過程において一方方向関数を用いることにより、同じ結果を生成する入力データを偽造することを困難にしている。また、生成されるデータサイズが大きいため、総当たり的な入力データの偽造も困難である。「メッセージダイジェスト」という名称は、暗号関連においては一般的な名称であり、良く知られた方式である。Ｓｉｇ（S_U）はメッセージダイジェスト処理関数をf_{md}とし、対象とするデータの複合操作を算術和で表現するとし、S_Uを用いた署名を関数S_Uで表現するとすると、次の処理を施した結果となる。

【００９５】

【数１】

$$S_U(f_{md}(L_G+P_G+P_U+\sum_{i=1}^{n}(L_{Mi}+P_{Mi}(S_G)+L_{Ui}+P_{Ui}(S_U))))$$

【００９６】$S_{U'}$：前バージョンのS_U

利用する公開鍵暗号システムに応じた秘密鍵であり、一般に５１２ビットから２０４８ビット程度の固定長のデータ列である。直前のバージョンの変更用秘密鍵である。機能は、S_Uと同様である（詳細は、P_Uの説明参照）。

【００９７】Ｓｉｇ（$S_{U'}$）：全体に対する$S_{U'}$による署名

署名を示すデータ列である。ここで全体とは、L_G、P_G、Ｖ、Ｆ、P_U、L_{Mi}、P_{Mi}（S_G）、L_{Ui}、P_{Ui}（S_U）、Ｓｉｇ（S_U）である。これは、新規に作成された場合には、付与されない。Ｓｉｇ（S_U）と同様に表記すると、次のように表せる。

【００９８】

【数２】

$$S_U(f_{md}(L_G+P_G+P_U+\sum_{i=1}^{n}(L_{Mi}+P_{Mi}(S_G)+L_{Ui}+P_{Ui}(S_U)+Sig(S_U))))$$

【００９９】なお、本実施例ではデータ全体に対して署名を行うようにしたが、改竄を防ぎたい一部データに対して署名を行うようにしてもよい。

【０１００】［公開錠リスト］図５に本実施例における公開錠リストの構造を示す。公開錠リストとは各個人が独立に所有するもので、その個人が信用しているグループ錠および個人錠を、その錠のラベルをインデックスとした配列で保持するものである。

【０１０１】図５に示すように、公開錠リストは、Ｇｉ：信用しているグループ錠、L_{Gi}：グループ錠Ｇｉのラベル、Ｉｉ：信用している個人の公開鍵、L_{Ii}：個人の公開鍵Ｉｉに対応するラベルから構成される。

【０１０２】公開錠リストへの新たなデータの追加の際に必要な錠の信用は、本実施例においては公開錠リストの所有者の判断に任されるものとする。ただし、既に信用しているグループ錠の次バージョンの自動信用は行うこととする。前述の信用レベルに関する演算規則を用いて信用できる錠あるいは信用体を決定することも可能である。この場合前述の公証局に登録された信用関係を利用することにより確実かつ容易に信用レベルを求めることが可能となる。

【０１０３】暗号化の際に、復号可能なグループおよび個人を指定するが、それは対応するグループ錠もしくは個人錠を１個以上、この公開錠リストから選択することにより指定する。

【０１０４】署名の正当性を確認する際には、署名時に

用いられた秘密鍵に対応する公開鍵をこの公開錠リストから取り出して利用する。

【０１０５】［秘密錠リスト］図６に本実施例における秘密錠リストの構造を示す。秘密錠リストとは各個人が独立に所有するもので、その個人が秘密鍵を獲得できるグループ錠を、そのグループ錠のラベルをインデックスとした配列で保持するものである。秘密鍵の獲得は、その個人の個人秘密鍵を、グループ錠に直接もしくは間接に適用することにより行われる。

【０１０６】図６に示すように、秘密錠リストは、Ｇｉ：秘密鍵が利用可能なグループ錠、、L_{Gi}：グループ錠Ｇｉのラベルから構成される。

【０１０７】秘密錠リストへの追加は、公開錠リストへのグループ錠の追加処理の中で、自身の個人秘密鍵を直接もしくは間接に適用することによりそのグループ錠内部のグループ秘密鍵を獲得可能であるならば追加することにより行う。よって利用者は追加処理を意識する必要はない。自身の個人秘密鍵により、そのグループ錠内部のグループ秘密鍵が獲得できるからといって、そのグループ錠を信用する根拠にはならないことには注意が必要である。

【０１０８】復号の際に、復号可能性の判断を秘密錠リストを用いることにより高速化する。また、実際の復号処理においても、必要なグループ秘密鍵の獲得処理にこの秘密錠リストを利用する。

【０１０９】署名の際には、自身の個人秘密鍵を用いる以外にも、この秘密錠リスト中のグループ秘密鍵を用いて署名することができる。このようにすれば、暗号文の受け手側で送り手の個人やグループを識別することができる。また、署名とともに署名に用いた秘密錠の公開鍵を添付すると署名の確認が容易になるとともに、署名を確認することなく公開鍵のみで送り手を容易に確認することができる。

【０１１０】［暗号］本実施例における暗号の構造を図７に示す。本実施例においては、グループ錠のL_{Mi}と$P_{Mi}(S_G)$のペアのリストと同様の構造を持たせることにより、複数の秘密鍵のいずれかを用いることにより復号可能としている。これにより、複数人に開示したい情報を暗号化する際に、必ずしもグループ錠を作成する必要をなくしている。すなわち、公開錠リストから任意に選択した個人やグループで構成される受け手のグループを一時的に作成することができる。

【０１１１】図７中の各記号の意味を以下に説明する。

Ｐｉ：復号できるグループ錠もしくは個人の公開鍵

利用する公開鍵暗号システムに応じた公開鍵であり、一般に５１２ビットから２０４８ビット程度の固定長のデータ列である。

【０１１２】Ｌｉ：Ｐｉのラベル

文字列である。

【０１１３】Ｄ：平文（機密を保持すべき情報）

任意のデータ列である。

【０１１４】Ｋ：平文Ｄを暗号化した共通鍵

公開鍵暗号は、暗号化処理および復号処理が遅いため、共通鍵暗号で平文を暗号化し、その共通鍵のみを公開鍵暗号により暗号化するハイブリッド方式を採用することが一般的である。このＫは、その共通鍵である。本実施例においては、ＫをＰｉでそれぞれ暗号化することにより、複数のグループもしくは個人による復号を可能とする。

【０１１５】Ｐｉ（Ｋ）：Ｐｉで暗号化したＫ

Ｋ（Ｄ）：で暗号化したＤ

【０１１６】Ｓ：暗号化処理を行った人が利用可能な秘密鍵

暗号に署名を付与する際に用いる、秘密鍵である。自身の個人秘密鍵か、秘密錠リストに含まれているグループ錠の秘密鍵のうちの１つを用いる。

【０１１７】Ｐ：署名に用いた秘密鍵Ｓと対になる公開鍵Ｐ

署名の確認の際には、署名者が署名に用いたと主張する秘密鍵に対応する公開鍵を利用する。その公開鍵を特定するために保持する。暗号文の受け手側においてその公開鍵が自身の公開錠リストに含まれていれば、自身が信用しているグループもしくは個人により署名されていることを確認することができ、暗号文の発信者または発信したグループを確認することができる。

【０１１８】Ｓｉｇ（Ｓ）：全体に対するＳによる署名

署名を示すデータ列である。ここで全体とは、Ｌｉ、Ｐｉ（Ｋ）、Ｋ（Ｄ）である。署名に関しては、グループ錠の構造のＳｉｇ（S_U）の項を参照。同様の表記に従えば、Ｓｉｇ（Ｓ）は次のように表せるものである。

【０１１９】

【数３】

$$S\left(f_{sd}\left(\sum_{i=1}^{\bullet}\left(Li+Pi\left(K\right)\right)D\right)\right)$$

【０１２０】［処理の流れ］本実施例の具体的な処理の流れを以下、図８から図１６に示されるフローチャートによって説明する。

【０１２１】［グループ錠生成］グループ錠生成についてのフローを図８に示す。グループを作成するとき（追加変更するときも同様）には、新しく指定するメンバに対応するグループ錠もしくは個人の公開鍵は作成者が信用している必要がある。そのため、新しく指定するメンバのグループ錠もしくは個人の公開鍵を信用していないときには、グループ錠の作成に先立って、信用すること、すなわち錠リストへの追加を行わなければならない。

【０１２２】作成したグループ錠は、まず自身の錠リストに追加される。錠リストとは、公開錠リストと秘密錠リストの総称である。さらに必要な者（作成したグルー

ブ向けに暗号化された暗号を復号する際に、グループのメンバはこのグループ錠が必要である。逆にこのグループ向けに暗号化する際にもグループ錠が必要となる。暗号化は任意の人が行える。そのためメンバおよびこのグループ向けの暗号化を行う可能性のある人への配布が必要となる）へ配布する。離れたセンタで保管し、暗号文の送り手や受け手の必要に応じて複合錠を送ったり、複合錠の必要な情報のみを送るようにしてもよい。本実施例においては、配布機構の説明は省略する。

【０１２３】図８のフローについて詳細に説明する。まずステップ１０１において生成するグループ錠のラベルを入力する。ステップ１０２では、入力されたラベルと同じラベルの錠がすでに錠リスト中にあるかが検討される。重複するラベルの錠の作成は拒否されることになり、すでに錠リスト中に同じラベルのものがある場合はステップ１１３に進みグループ錠の作成が中止される。同じラベルのものが無い場合は、ステップ１０３に進む。

【０１２４】ステップ１０３およびステップ１０４では、メンバＭｉと変更権所有者Ｕｉが指定される。メンバは、このグループ錠を使用した暗号システムを利用するメンバであり、変更権所有者は、このグループ錠の変更、例えばメンバの追加、削除等を行う権利を有する者である。メンバ、および変更権所有者は、いずれも個人に限らずグループでの登録が可能であり、グループ錠生成者が有する公開錠リストの中から１つ以上のグループ錠もしくは個人の公開鍵を選択して指定される。

【０１２５】ステップ１０５では、生成されるグループ錠の秘密鍵S_Gと公開鍵P_Gを生成する。ステップ１０６では、生成された秘密鍵S_GをメンバＭｉのそれぞれの公開鍵P_{Mi}で暗号化したP_{Mi}（S_G）を生成し、それぞれにラベルL_{Mi}を対応させる。

【０１２６】ステップ１０７では、生成するグループ錠の変更用秘密鍵S_Uと変更用公開鍵P_Uが生成される。ステップ１０８では、生成されたグループ錠変更用秘密鍵S_Uを変更権所有者の公開鍵P_{Ui}によって暗号化し、P_{Ui}（S_G）を生成し、それぞれにラベルL_{Ui}を対応させる。

【０１２７】ステップ１０９では、生成されるグループ錠のバージョン番号を設定する。ステップ１１０では、それぞれのステップで生成された、L_G，P_G，S_G，S_U，P_U，Ｖ，P_{Mi}（S_G），P_{Ui}（S_U）の各データを一体とする。ステップ１１１では、一体となった前データに対する変更用秘密鍵S_Uによる署名、すなわちデータ変換が実行される。ステップ１１２でグループ錠生成者の錠リストにグループ錠を登録追加することでグループ錠の生成が終了する。生成されたグループ錠は先に説明した図４に示す構成を有する。

【０１２８】［錠リストへの追加］図９に錠リストへの追加手続のフローを示す。錠リストへの追加は、信用できるグループ錠もしくは個人の公開鍵だけについて行われる。この処理は、自身が生成および変更（新しいバージョンの作成）したグループ錠の追加、他者から得たグループ錠の追加のいずれにおいても用いられる。

【０１２９】本実施例では、公証局を用いて鍵を配布したり、電子メールやフロッピを介して鍵を配布したりという配布に関する処理は含めていない。また、鍵に対する署名を利用し、その署名者に対する信頼度、署名者の鍵に対する信用度の演算を行い、鍵の信用度を算出するような処理は省略してある。前述した信用度の演算による信用度レベルの獲得をこのフロー中に含め、信用度の判断に用いることは可能である。本実施例においては、既に信用しているグループ錠の新しいバージョンの自動的な信用手続きについては示してある。ここでは、新しいバージョンが、直前のバージョンの変更用秘密鍵によって署名されていることが確認できた場合にのみ自動的に信用している。

【０１３０】秘密錠リストへの追加は、信用できたグループ錠の中から、自身の個人秘密鍵を用いることにより直接もしくは間接に、そのグループ錠の秘密鍵を獲得できるものだけを追加する。

【０１３１】図９に示すフローを詳細に説明する。ステップ２０１で追加する錠の指定が行われると、ステップ２０２，２０３，２０４において、直前のバージョンの錠の変更用秘密鍵S_U，による署名の有無、信用の有無、署名の正確性について判断され、いずれかが「いいえ」の場合に、ステップ２１４に進み、追加する錠を信用するか否かを、信用錠の所有者自身が判断して入力する。信用する場合は、ステップ２１０に進み、信用しない場合は、錠リストへの追加は実行しない。ステップ２１４および２１５において前述の信用度を獲得するための演算を用いることができる。

【０１３２】ステップ２０５～２０９は、以前のバージョンの扱いを決定するステップである。新しいバージョンのグループ鍵を追加するときには、以前のバージョンのグループ錠を適切に扱う必要がある。これは新しいバージョンのグループ鍵に含まれているＦの値により判断する。Ｆの値にかかわらず、以前のバージョンは古いため、新たに暗号化したり、署名したりすることは行ってはならない。そのため、公開錠リストや、秘密錠リストは、最新のものと、それ以外に分けておくべきである。本実施例においては、その分類は省略し、利用する際に最新という指定をするにとどめている。Ｆの値に応じた対応は次の通りである。

【０１３３】ａ）Ｆ＝「必要」の場合には、古いバージョンのグループ錠は残される。

ｂ）Ｆ＝「不要」の場合には、古いバージョンのグループ錠は削除される。

ｃ）Ｆ＝「抹消」の場合には、自身が新しいバージョンの秘密鍵を獲得できれば、残される。そうでなければ削

除される。

【０１３４】ステップ２１０～２１３は、公開錠リストへの追加を行い、追加される錠の秘密鍵の利用可能性を判断し、利用可能な場合には、秘密錠リストへの追加も併せて行うことを示すステップである。

【０１３５】［秘密錠の利用可能性判断］図１０に秘密鍵の利用可能性を判断するフローを示す。これは指定された任意のグループ錠の中に暗号化されて含まれている秘密鍵を、自身の個人秘密鍵を直接もしくは間接に適用することにより獲得することができるかどうかの判断を行う処理である。

【０１３６】この処理は、あるグループ錠を、秘密錠リストに含めて良いか否かの判断（図９のステップ２１２およびステップ２１３）に用いる。他にも、復号の際にグループ鍵を利用可能か否かを判断するためなどにおいて、この処理と同じ判断が必要である。しかし、秘密錠リストに含まれているグループ錠が、その時点において知っている限りにおいて、自身が秘密鍵を獲得できる全てのグループ錠であることを利用して、秘密錠リストに含まれているか否かという簡便な処理で済むことが多く、この処理を直接利用しなければならないことは多くない。

【０１３７】処理の内容は、まず自身の個人秘密鍵を直接用いて与えられたグループ錠の秘密鍵を獲得できるか否かを判断する。それで獲得できない場合には、自身の秘密錠リスト中の各グループ鍵を直接用いて与えられたグループ錠の秘密鍵を獲得できるか否かを判断する。秘密錠リスト中のグループ錠の秘密鍵を利用可能であることが判明しているので、判断するだけであれば、この手順で処理すれば良い。

【０１３８】図１０のフローを詳細に説明する。ステップ３０１では、判断の対象とするグループ錠を指定し、ステップ３０２で、自身の個人錠が判断対象であるグループ錠のメンバであるかが検討され、メンバであれば利用可能であるとされる。メンバでない場合は、ステップ３０３からステップ３０５において、現在の秘密錠リストの要素Ｇｉについて検討されＧｉが判断対象の鍵のメンバであるかが検討される。ステップ３０３，３０４，３０５は、Ｇｉのｉを順次インクリメントして繰り返し実行することを意味する。この繰り返しステップ中、いずれかのＧｉが判断対象の鍵のメンバである場合には、利用可能と判断される。

【０１３９】［暗号化］図１１に情報の暗号化処理フローを示す。ここで入力するべきものは次の３つである。

ａ）平文

ｂ）復号可能者

公開錠リストに含まれる最新のグループ錠もしくは個人の公開鍵を合わせて一つ以上指定する。

ｃ）署名者

自身の個人秘密鍵か、秘密錠リストに含まれる最新のグループ錠を一つだけ指定する。署名しなければ指定する必要はない。

【０１４０】署名とは、署名対象であるデータをメッセージダイジェストし、その結果である署名ブロックを秘密鍵によって署名することである。秘密鍵による署名とは、秘密鍵による暗号化である。詳細については、データ構造「暗号」と、データ構造「グループ錠」のＳｉｇ（S_g）の項参照。

【０１４１】図１１のフローについて詳細に説明する。ステップ４０１では、機密を保持する情報Ｄを入力し、ステップ４０２で、復号を可能とする最新のグループおよび個人に対応する公開鍵Ｐｉを、自身の公開錠リストから１つ以上選択する。これは、暗号化されたデータの復号を可能とするメンバを選択するものである。

【０１４２】ステップ４０３では、共通鍵Ｋを生成し、Ｋを鍵とする共通鍵暗号方式による情報Ｄの暗号化を実行する。これは前述の［暗号］の欄で述べたように、公開鍵暗号は、暗号化処理および復号処理が遅いため、共通鍵暗号で平文を暗号化し、その共通鍵のみを公開鍵暗号により暗号化するハイブリッド方式を採用していることによるものである。なお、この共通鍵Ｋは暗号化を行う毎に生成するものでなくてもよく、必要に応じて生成するものであったり、あるいは予め決められた固定的なものであってもよい。

【０１４３】ステップ４０４ではＫを各復号可能者の公開鍵Ｐｉで暗号化しＰｉ（Ｋ）を生成し、それぞれに対応するラベルを付与する。ステップ４０５でその生成された暗号に対する署名を行うか判断し、行わない場合は、ステップ４１０で各データのまとめを実行し、暗号化処理を終了する。署名を実行する場合は、ステップ４０６に進む。

【０１４４】ステップ４０６～４０９は署名の処理ステップであり、署名を行うデータのメッセージダイジェスト処理（ステップ４０６）を行い、署名用の鍵を秘密錠リストから選択（ステップ４０７）し、選択した秘密鍵による署名を実行（ステップ４０８）し、配列Ｋ（Ｄ）と署名済みメッセージダイジェスト（＝署名ブロック）をまとめる（ステップ４０９）処理である。以上のステップにより暗号化処理が終了する。

【０１４５】［復号可能性判断］図１２に任意の暗号を自身が復号可能であるか否かを判断する処理フローを示す。このフローは、例えば、暗号ファイルのリストをしたとき、自身が復号可能なものがどれであるのかを確認したいとき等に使用される。このフローは復号可能性の判断を高速に実行する処理である。具体的には、ラベルが一致しなければ復号できないことを利用し、まずラベルの一致を確認し、ラベルが一致した場合に限り復号を試みる。一般にラベルの選定方法を適切に決めれば、この方法で十分な性能が得られる。もしラベルの選定方法を規定できないならば、「暗号」にラベルだけでなく、

暗号化に利用した公開錠を付与することにより、高速化する方法もある。

【0146】処理は、まず自身の個人秘密鍵の適用を試み、復号できなければ自身の秘密錠リスト中の各グループ錠の適用を試みる。ここにおける復号は、「暗号」中のラベルLiに対応するPi（K）のみの復号である。ここでは、平文を得ることは目的ではないので、K（D）の復号は行わない。

【0147】図12の復号可能性判断フローについて詳細に説明する。ステップ501で復号可能性を判断する暗号を指定する。ステップ502、503で暗号中のラベルLiと自身の個人錠のラベルとの一致があるかが判断される。一致がある場合は、ステップ509へ進み、復号を試みる。ここで復号できない場合、およびステップ502、503において一致するラベルがなかった場合は、ステップ504、505において所有する秘密錠ラベルとの一致が判断される。一致するラベルL_{Gi}があったときは、ステップ511に進み、ラベルL_{Gi}に対応するGiの秘密鍵S_{Gi}を獲得し、ステップ512，513で復号を試みる。復号が成功しない場合は、ステップ506，507に進み、他の所有秘密錠リストのラベルとの一致および個人錠のラベルとの一致について調べることとなる。なお、ステップ506はステップ504と同一の処理を異なるラベルについて繰り返すことを示し、ステップ507はステップ502について異なるラベルについて繰り返すことを示している。ステップ510あるいは、ステップ513において復号できたときは、ステップ514で復号できるとの判断がなされる。

【0148】［グループ錠中の秘密鍵の獲得］図13に秘密錠リスト中に存在するグループ錠の秘密鍵S_Gを獲得するフローを示す。グループ錠の秘密鍵は暗号情報の復号や署名の際などに用いる。

【0149】秘密錠リストには、個人の秘密鍵を直接もしくは間接に適用することにより、その秘密鍵を獲得できるグループ錠のみが含まれているので、獲得できることは明らかである。

【0150】処理は、まず自身の個人秘密鍵を直接適用することを試みる。それが失敗した場合には、秘密錠リスト中のグループ錠を適用することを試みる。グループ錠の適用の試みにおいては、この処理を再帰的に呼び出す。グループをノードとし、メンバというグループ間の包含関係を有向アークとして形成される有向グラフは、ループを持たない。よって、この処理で秘密鍵を獲得することができる。

【0151】図13の秘密鍵S_{Gi}の獲得フローについて詳細に説明する。まずステップ601で秘密錠リスト中のグループ錠Giを指定する。ステップ602で自身の個人錠がグループ錠Giのメンバに含まれるかが検討され、含まれる場合は、ステップ607に進み、グループ錠Gi中にある個人公開鍵でグループ秘密鍵を暗号化したPMj（S_G）を抽出し、これを個人秘密鍵で復号し、グループ秘密鍵S_Gを獲得する。

【0152】ステップ602において、自身の個人錠がグループ錠Giのメンバに含まれない場合は、ステップ603～605において、秘密錠リストのすべての要素Gkにたいして、GkがGiのメンバであるかが検討される。これは、自身の保有する「秘密錠が利用可能なグループ錠Gk」各々について、グループ錠Giのメンバとして含まれているかを検討するステップである。ステップ604でグループ錠Giのメンバであるが検出されたときは、ステップ608でGkの秘密鍵S_{Gk}を獲得し、ステップ609でグループ錠Gi中にある暗号化したPMj（S_G）を抽出し、これを秘密鍵S_{Gk}で復号し、グループ秘密鍵S_Gを獲得する。

【0153】［復号］図14に任意の暗号を復号する際のフローを示す。図14に示すフローは、前述した「復号可能性判断」処理とほぼ等しいフローである。ステップ701～713は、図12の復号可能性判断フロー中のステップ501～513に対応する。ただし、ステップ714において、共通鍵暗号の鍵Kを用いて、K（D）を復号し、平文Dを獲得する。暗号が署名がされている場合、必要ならば、平文Dを獲得するとともに、署名の確認を行う。

【0154】［署名確認］図15に署名確認のフローを示す。署名対象にメッセージダイジェスト処理を施した結果と、署名ブロック（署名処理により付与されたデータ）を署名の際に用いられたとされる秘密鍵に対応する公開鍵で復号した結果と比較する。その2つの結果が等しければ署名が正しくなされ、署名対象が改竄されていないことが確認できる。

【0155】ただし、署名に用いられた秘密鍵に対応する公開鍵を信用していなければならない。自身の公開錠リストに含まれていれば良い。信用していなければ、署名の確認はできない。

【0156】メッセージダイジェストの結果と、復号した結果が等しくないときには、署名対象が改竄されていることが分かる。

【0157】図15に示す署名確認フローについて説明する。まずステップ801で、署名対象をメッセージダイジェストする。メッセージダイジェストとは前述のように、署名の対象範囲を全て暗号化するにはコストがかかるために、対象範囲のデータサイズと独立に、対象範囲の内容に応じて128ビット程度の情報を生成する処理である。次にステップ802において、署名に使用する秘密鍵に対応する公開鍵の信用について判断する。公開鍵を信用していない場合は、ステップ806で署名確認は不可能と判断される。

【0158】ステップ802において、公開鍵の信用性が確認されれば、ステップ803に進み、署名ブロックを署名の際に用いられたとされる秘密鍵に対応する公開

鍵で復号し、ステップ８０４とでメッセージダイジェストとの同一性判断がなされる。これが実際上の署名確認ステップとなる。このステップ８０４において同一性がないと判断されればステップ８０７において署名は正しいものではない。すなわち、署名を行った秘密鍵は正しいものではないと判断される。ステップ８０４においてメッセージダイジェストと復号結果が等しいと判断されれば、ステップ８０５においてその署名は正当に行われたと結論づけられる。

【０１５９】［グループ錠変更］図１６にグループ錠の変更フローについて示す。グループ錠の変更には、次の４種類がある。フローチャートにおいて、４本の処理に分岐している部分の左側からの順序で示す。

【０１６０】Ａ．今から追加

新たにメンバを追加する。追加された新たなメンバは、追加以前に暗号化された暗号を復号することはできない。この場合には、新しい秘密鍵と公開鍵の対を新しいバージョンのグループ錠のS_GとP_Gとする。また、Ｆの値は「必要」となる。よって、新しいバージョンを受け取った個人は、以前のバージョンを削除しない。これは、追加以前に暗号化された暗号を、以前からのメンバが復号するために必要であるためである。

【０１６１】Ｂ．遡って追加

新たにメンバを追加する。追加された新たなメンバは、追加以前に暗号化された暗号も復号することができる。この場合には、以前のS_GとP_Gをそのまま利用する。そのため、Ｆの値は「不要」となる。よって、新しいバージョンを受け取った個人は、以前のバージョンを削除する。以前に暗号化された暗号を復号する場合にも新しいバージョンを用いれば良い。

【０１６２】Ｃ．今から削除

既存のメンバを削除する。削除されたメンバは、削除以前に暗号化された暗号を復号することができる。当然、削除以降に暗号化されたものは復号できない。この場合には、新しい秘密鍵と公開鍵の対を新しいバージョンのグループ錠のS_GとP_Gとする。また、Ｆの値は「必要」となる。よって、新しいバージョンを受け取った個人は、以前のバージョンを削除しない。これは、削除以前に暗号化された暗号を、削除されたメンバも含めた以前のメンバが復号するために必要であるためである。

【０１６３】Ｄ．遡って削除

既存のメンバを削除する。削除されたメンバは、削除以前に暗号化された暗号も復号することができない。この場合には、新しい秘密鍵と公開鍵の対を新しいバージョンのグループ錠のS_GとP_Gとする。また、Ｆの値は「抹消」となる。よって新しいバージョンを受け取った個人は、以前のバージョンを削除しない。これは、削除以前に暗号化された暗号を、削除されたメンバを除いた以前のメンバが復号するために必要であるためである。ただし、受け取った個人が新しいバージョンの秘密鍵を獲得できない場合、すなわち削除されたメンバであった場合には、削除する。これは、削除以前に暗号化された暗号も削除されたメンバが復号できないようにするためである。この削除されたメンバが以前のバージョンのグループ錠を削除することは数学的に保証するものではなく、システムとして削除を促進することはできるという性格のものである。

【０１６４】グループ錠を変更したときには、Ｆの値が意味を持つだけでなく、以前のバージョンの変更用秘密鍵で署名する。これは前述したように、以前のバージョンを信用している場合に、新しいバージョンを自動的に信用できるようにするためである。グループ錠を変更したときには、必要な者に速やかに配布する。

【０１６５】図１６および図１７に示すグループ錠変更フローについて詳述する。ステップ９０１、９０２において変更するグループ錠を特定し、変更の種類を判別する。ステップ９０２において追加と削除の処理のいずれかを選択することとなるが、メンバの入れ替えのように追加、削除が同時に発生するような場合は、メンバごとに順序を設定して１メンバごとに処理を実行する。

【０１６６】ステップ９０２において変更がメンバの追加である場合は、ステップ９０３へ進み、公開錠リストから追加するメンバに対応するグループもしくは個人の公開鍵を選択する。次にステップ９０４においてこの追加が現在からの追加でよいか、あるいは過去に遡って追加する必要があるかについて判断される。すなわち、過去の暗号情報の復号を可能とするか否かについてを決定するものである。ステップ９０４の判断が「いいえ」すなわち現時点以降の追加となる場合は、ステップ９０５でグループ公開鍵P_Gとグループ秘密鍵S_Gが生成され、ステップ９０６でグループ錠の直前バージョン扱いを示す「Ｆ」を必要と設定する。これは、新たなバージョンのグループ錠と元の旧バージョンのグループ錠が共存することを示している。一方ステップ９０４の判断が「遡って追加」である場合は、ステップ９０７、９０８へ進み、現在変更中のグループ錠のS_G、P_Gをそのまま変更されたグループ錠のS_G、P_Gとして設定し、Ｆを「不要」と設定する。これは、旧バージョンのグループ錠が新バージョンのグループ錠に完全に置き換えられたことを示している。次にステップ９０９で、グループ秘密鍵S_Gを追加メンバを含めたメンバの公開鍵P_{Mi}で暗号化し、P_{Mi}に対応するラベルL_{Mi}をインデックスとする$P_{Mi}（S_G）$の配列を形成する。

【０１６７】次にステップ９１０で新しい変更権所有者の設定、ステップ９１１で変更鍵の秘密鍵と公開鍵のペアの生成、ステップ９１２で新たな変更権所有者の公開鍵を用いて変更鍵の秘密鍵を暗号化する。

【０１６８】さらに、ステップ９１３でバージョン番号Ｖの更新、ステップ９１４で各データの一体化、ステップ９１５で一体化されたデータに対する変更秘密鍵によ

る署名を実行し、署名結果Ｓｉｇ（S_U）とし、ステップ９１６でさらに署名結果を加えたデータの一体化を行う。ステップ９１７で、変更前バージョンの変更用秘密鍵$S_{U'}$で署名し、Ｓｉｇ（$S_{U'}$）とし、ステップ９１８で変更されたグループ錠を作成者の信用錠リストに追加してグループ錠の変更手続を終了する。

【０１６９】ステップ９０２において変更がメンバの削除である場合は、ステップ９１９へ進み、削除するメンバを選択する。次にステップ９２０においてこの削除が現在からでよいか、あるいは過去に溯る必要があるかについて判断される。すなわち、過去の暗号情報の復号を可能とするか否かについてを決定するものである。ステップ９２０の判断が「いいえ」すなわち現時点以降の削除となる場合は、ステップ９２１でグループ公開鍵P_Gとグループ秘密鍵S_Gが生成され、ステップ９２２でグループ錠の直前バージョン扱いを示す「Ｆ」を必要と設定する。これは、新たなバージョンのグループ錠と元の旧バージョンのグループ錠が共存することを示している。一方ステップ９２０の判断が「溯って削除」である場合は、ステップ９２３、９２４へ進み、現在変更中のグループ錠のS_G、P_Gをそのまま変更されたグループ錠のS_G、P_Gとして設定し、Ｆを「抹消」と設定する。次にステップ９２５で、グループ秘密鍵S_Gを削除メンバを削除したたメンバの公開鍵P_{Mi}で暗号化し、P_{Mi}に対応するラベルL_{Mi}をインデックスとするP_{Mi}（S_G）の配列を形成する。以下の手続きであるステップ９１０以降は追加の場合と同様である。

【０１７０】以上、本発明の実施例を説明したが、例えば複号錠の生成、あるいは変更は、暗号化装置、復号装置、あるいはその他の第３局における装置等いずれにおいて実行されてもよく、他のこの公開鍵暗号方式において用いられる他の構成要素、例えば各種の錠リスト等についても同様である。

【０１７１】

【発明の効果】以上説明したように、本発明のグループ型公開鍵暗号方式においては、従来の個人を単位とする公開鍵暗号方式にグループの概念を導入し、グループに属する任意のメンバによる平文の暗号化処理、および暗号情報の復号処理をグループを単位として生成されたグループ公開鍵、グループ秘密鍵、および個人の公開鍵および秘密鍵とを組み合わせて用いることによって実行可能とした。この構成により、グループ内と外との間では高度な機密性を保ちながら、グループ内のメンバ間ではメンバであることの確認の基に暗号情報を共有することを可能とした。また、グループに属するメンバによる電子署名により、グループ内のメンバによる正当な暗号化処理およびその確認を可能とした。

【０１７２】さらに、本発明のグループ型公開鍵暗号方式では、グループを構成するメンバの変更に対するグループ錠の変更に際し、グループ公開鍵およびグループ秘密鍵の新たなペアの生成および登録を、メンバの変更時点に応じて実行する構成とし、メンバ変更に対してグループ錠を柔軟に変更できる構成とした。また、グループ錠変更に際しての署名をグループ錠を構成する要素の配列全体に対して行うように設定し、変更の保証を確実なものにした。

【図面の簡単な説明】

【図１】　複合錠の信用レベルを決定する演算規則を示した図である。

【図２】　信用体に対する信用レベルとその信用体が有する他のものへの信用レベルから、該他のものの信用レベルを決定するの演算規則を示す図である。

【図３】　本発明の暗号方式全体の概要を示す構成図である。

【図４】　本発明のグループ錠の構成を示す図である。

【図５】　本発明の公開錠リストの構成を示す図である。

【図６】　本発明の秘密錠リストの構成を示す図である。

【図７】　本発明の暗号の構成を示す図である。

【図８】　本発明のグループ錠生成フローを示す図である。

【図９】　本発明の錠リストへの追加フローを示す図である。

【図１０】　本発明の秘密錠の利用可能性判断フローを示す図である。

【図１１】　本発明の暗号化フローを示す図である。

【図１２】　本発明の復号可能性判断フローを示す図である。

【図１３】　本発明の秘密錠リスト中の秘密鍵の獲得フローを示す図である。

【図１４】　本発明の復号フローを示す図である。

【図１５】　本発明の署名確認フローを示す図である。

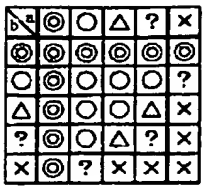
【図１６】　本発明のグループ錠変更フローを示す図（その１）である。

【図１７】　本発明のグループ錠変更フローを示す図（その２）である。

【符号の説明】

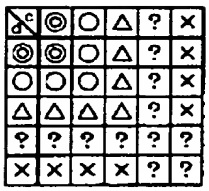
１０１　　個人
１０２　　平文
１０３　　暗号
１０４　　錠リスト
１０５　　個人秘密鍵

【図1】



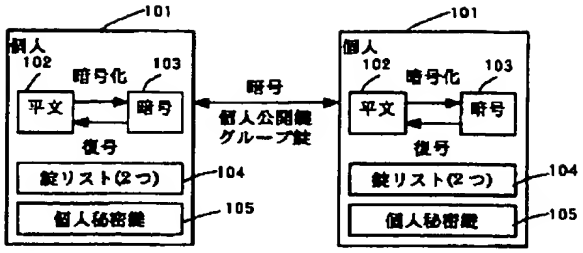
a：個人Aの信用レベル
b：個人Bの信用レベル

【図2】

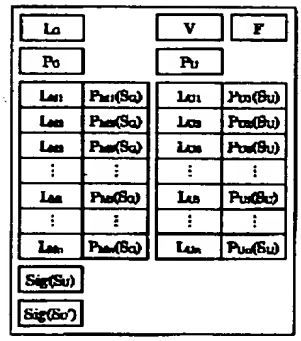


c：信用体に対する信用レベル
d：その信用体の他の信用体に対する信用レベル

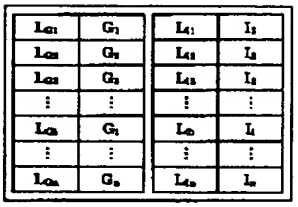
【図3】



【図4】

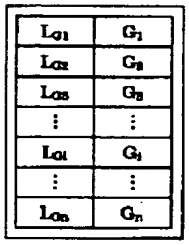


【図5】



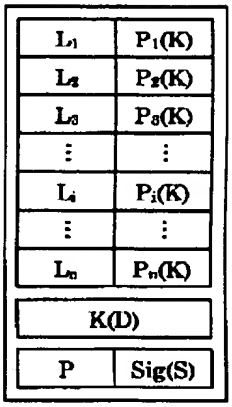
Gi：　信用しているグループ鍵
Lci：　グループ鍵 Giのラベル
Ij：　信用している個人の公開鍵
Lij：　個人の公開鍵 Ijに対応するラベル

【図6】

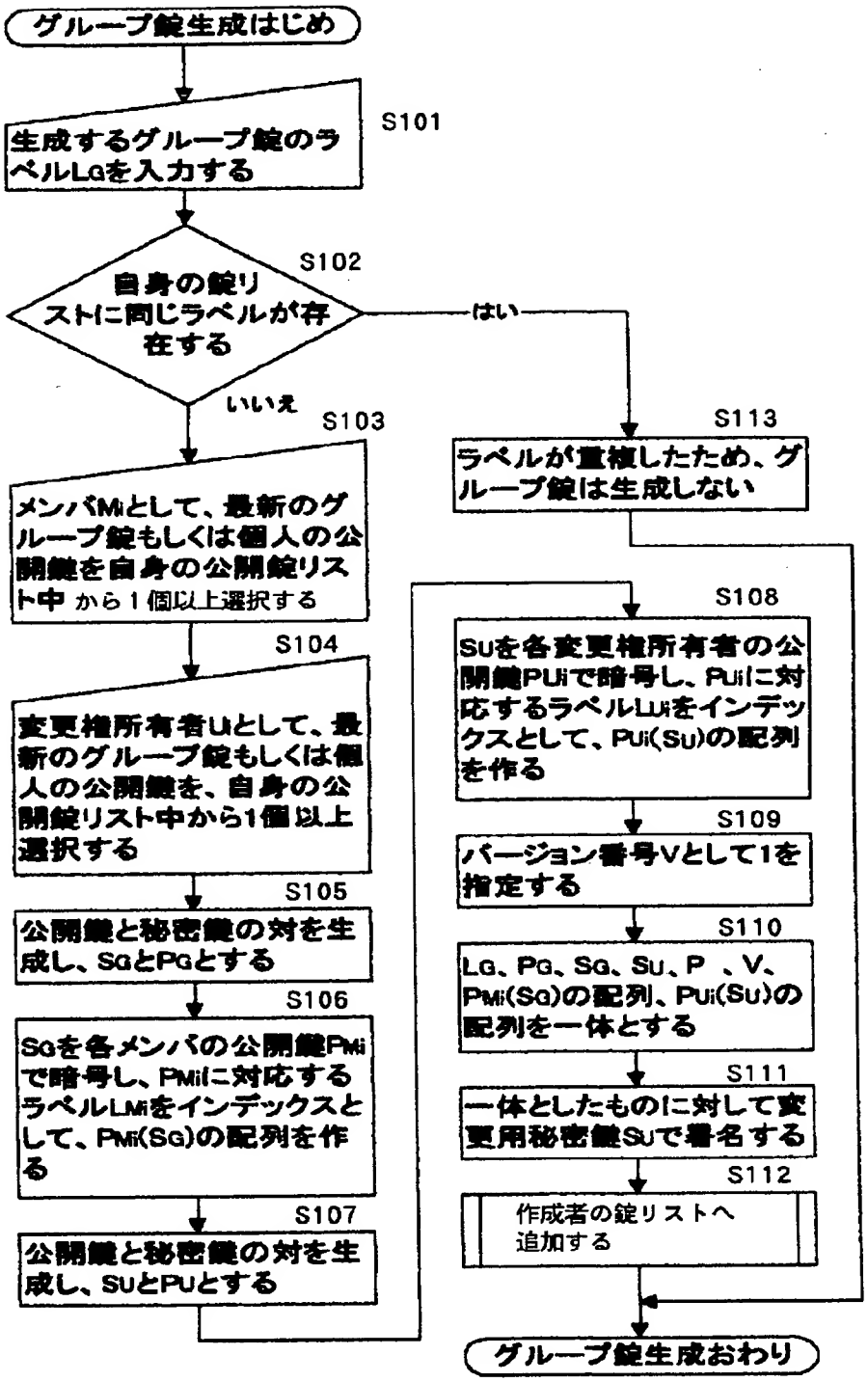


Gi：　秘密鍵が利用可能なグループ鍵
Lci：　グループ鍵 Giのラベル

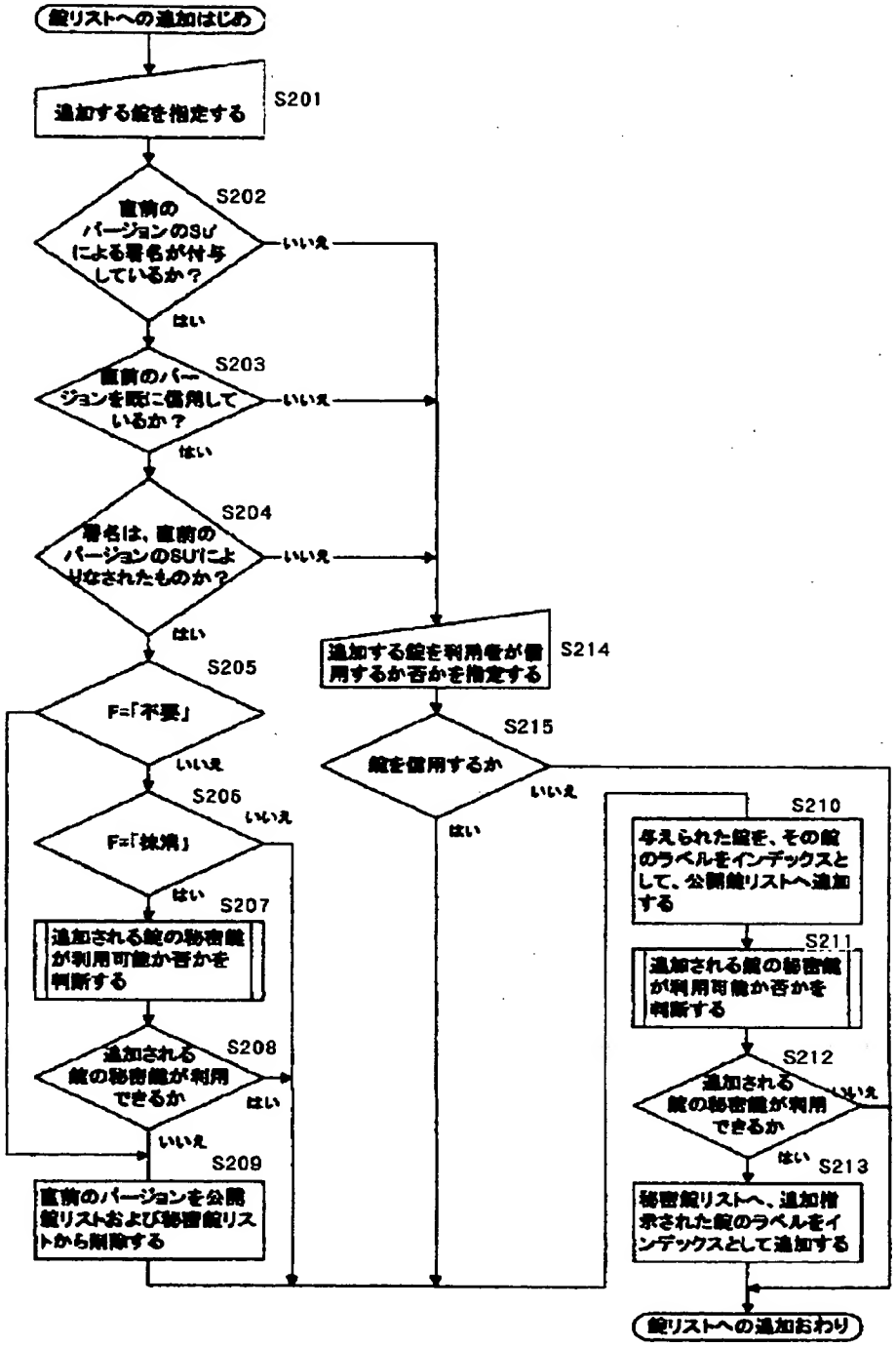
【図7】



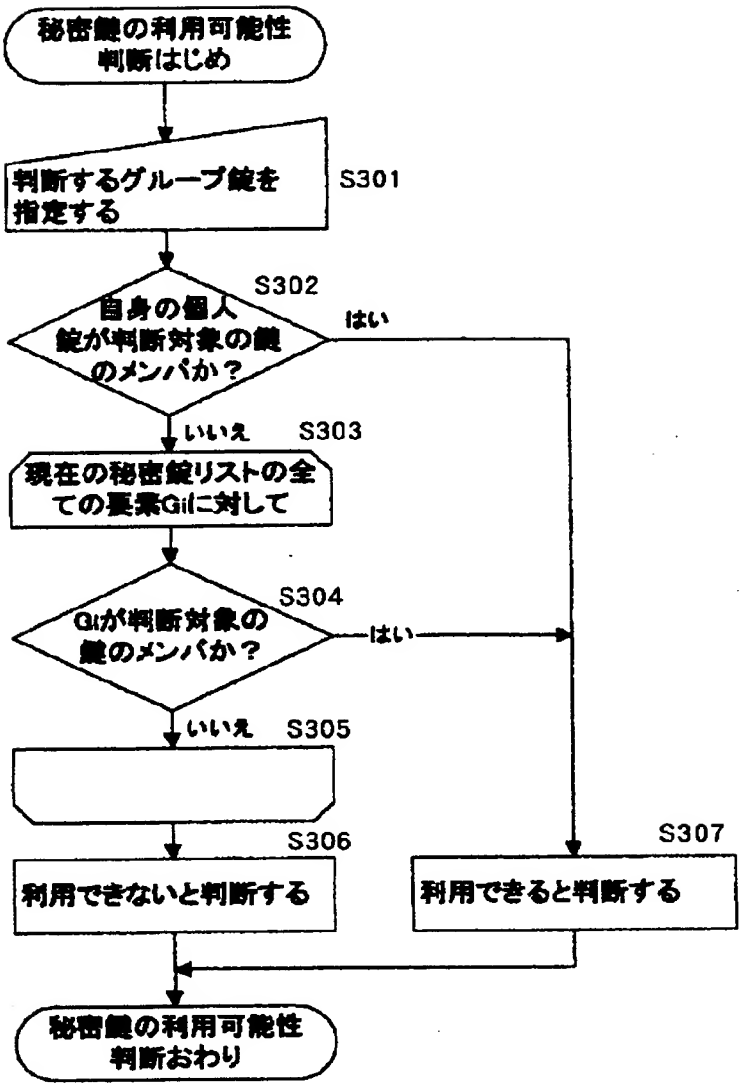
【図8】



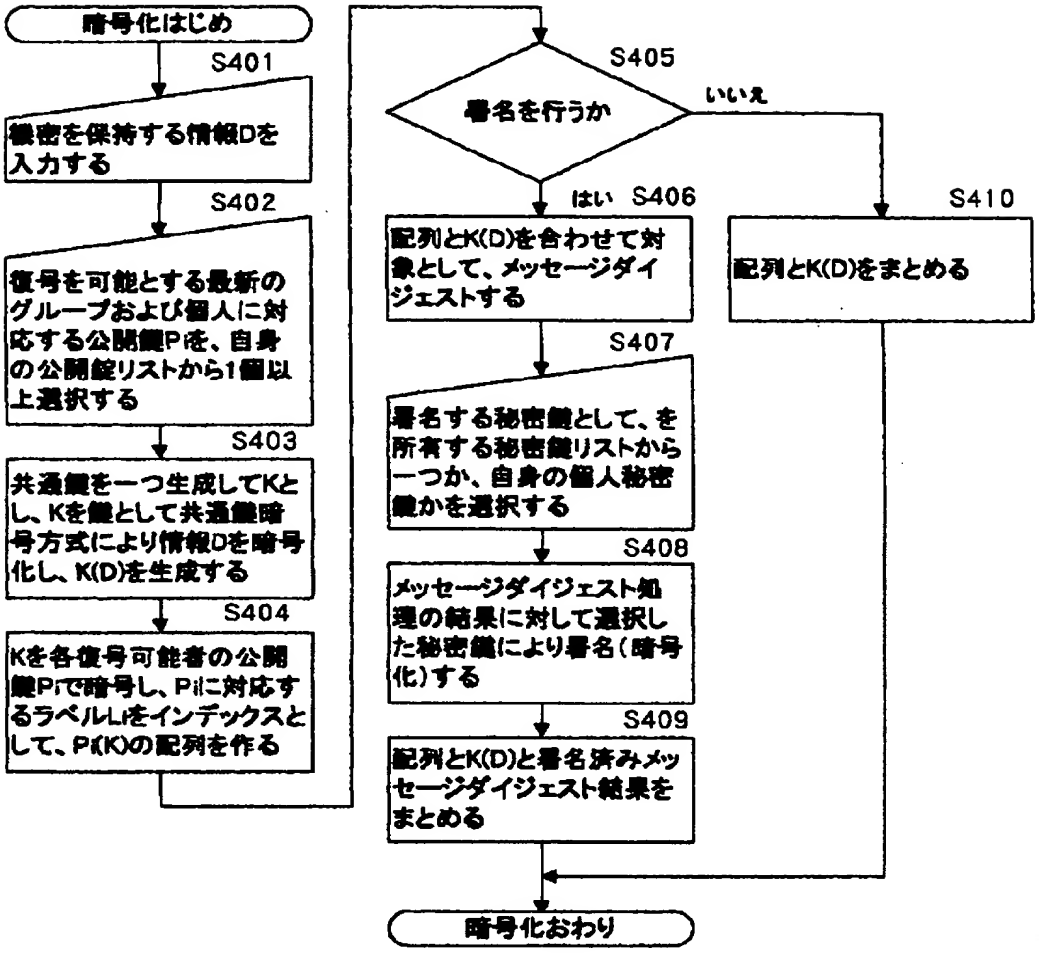
【図９】



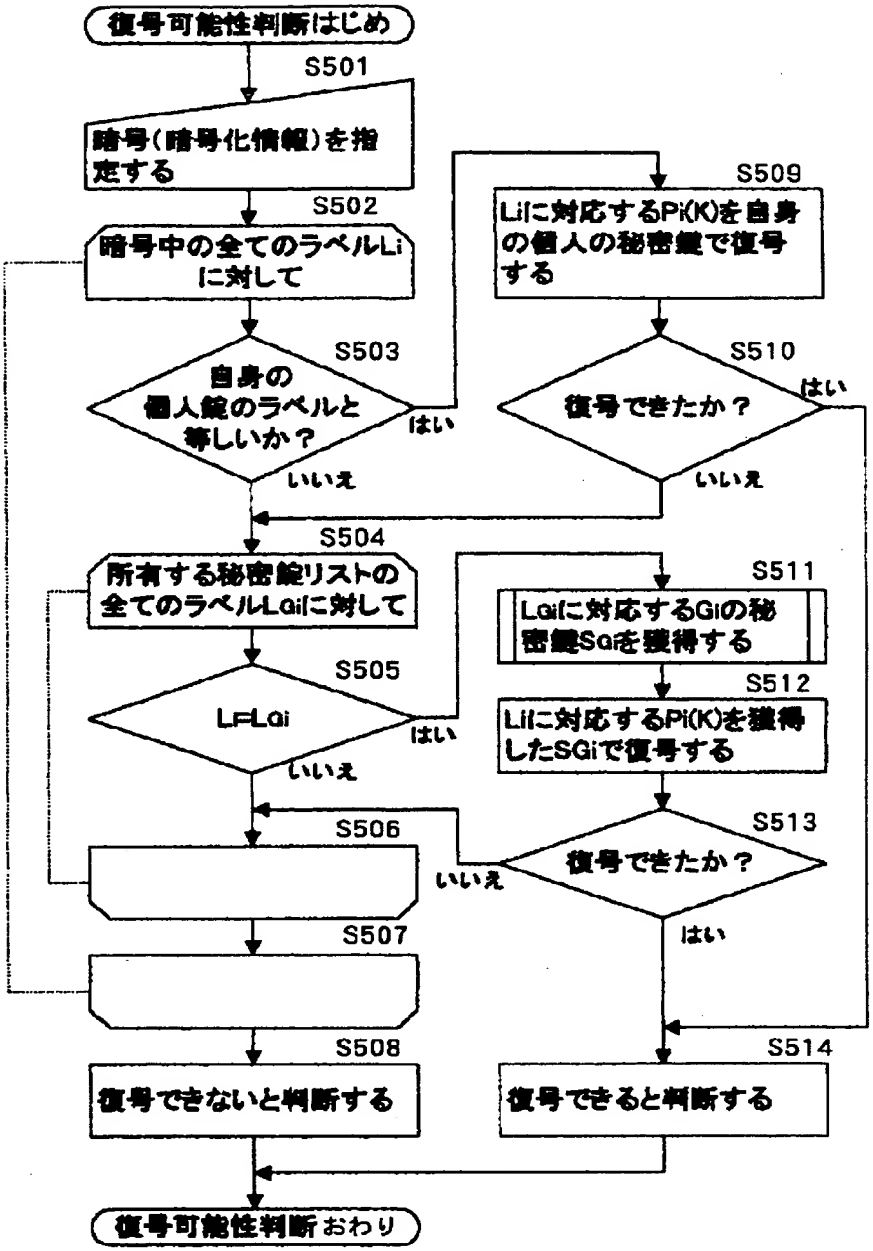
【図１０】



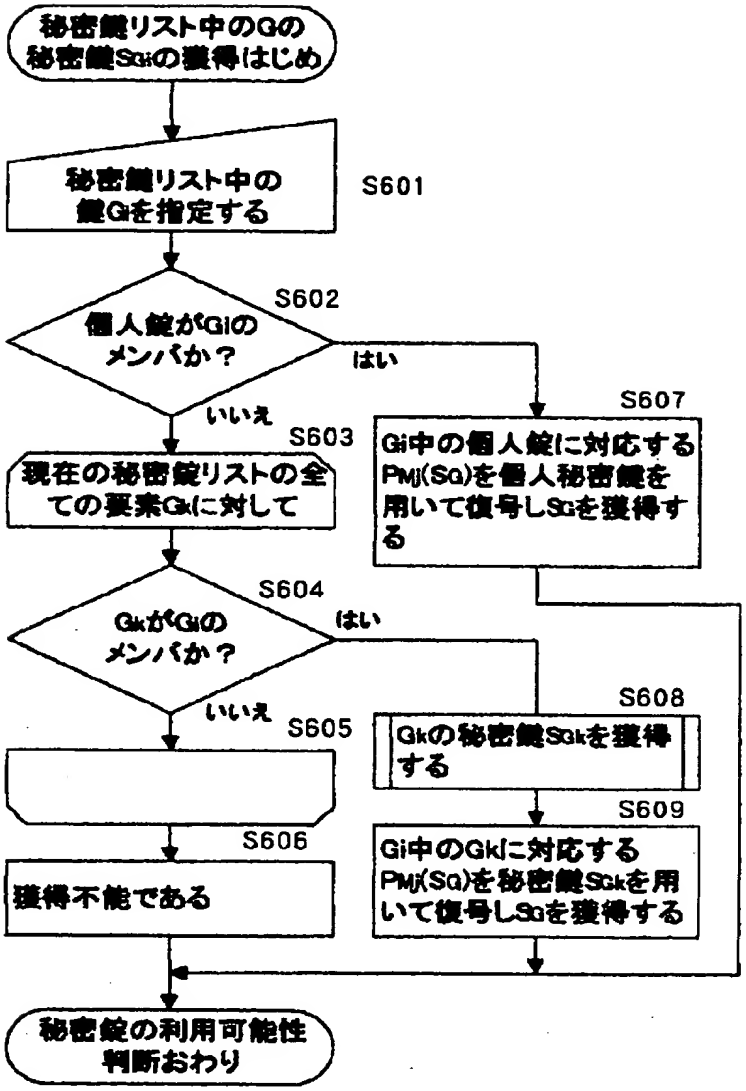
【図11】



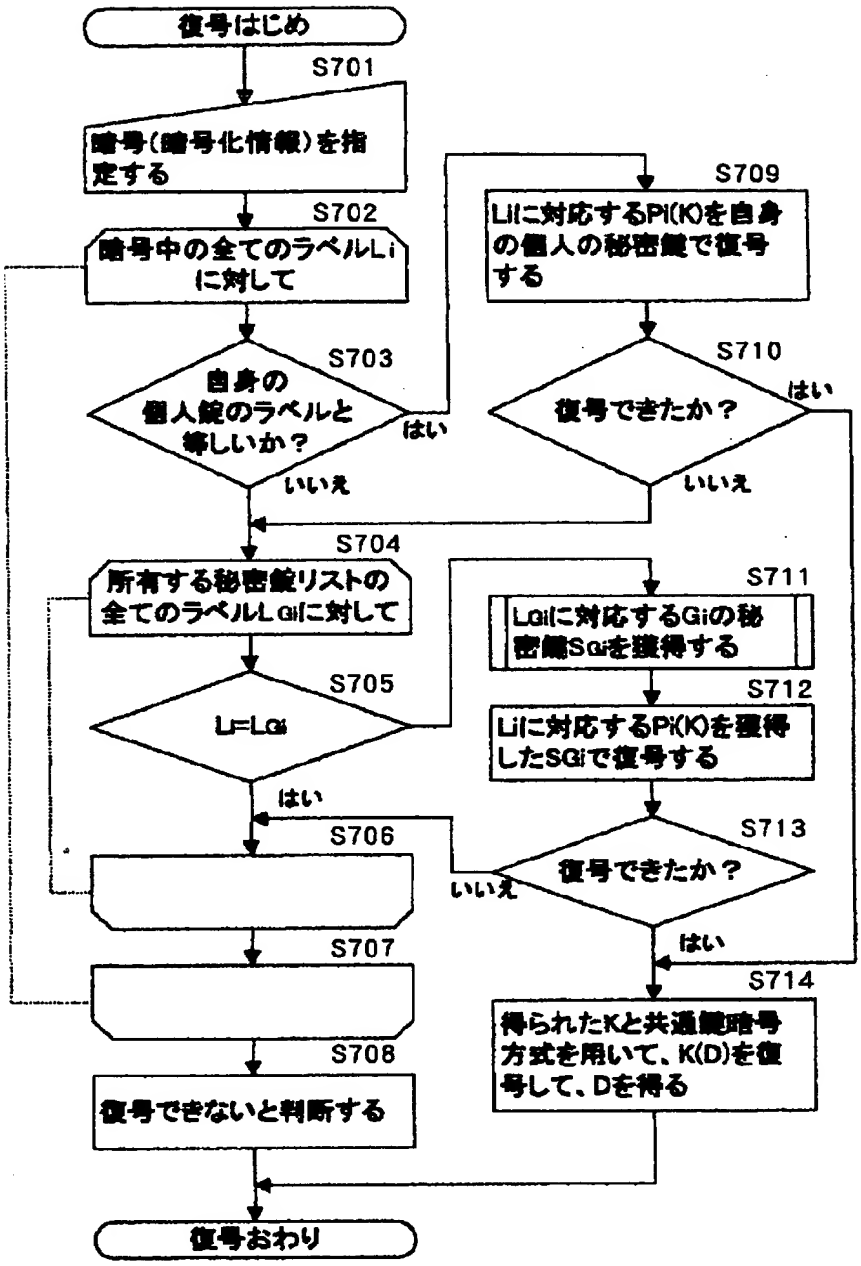
【図12】



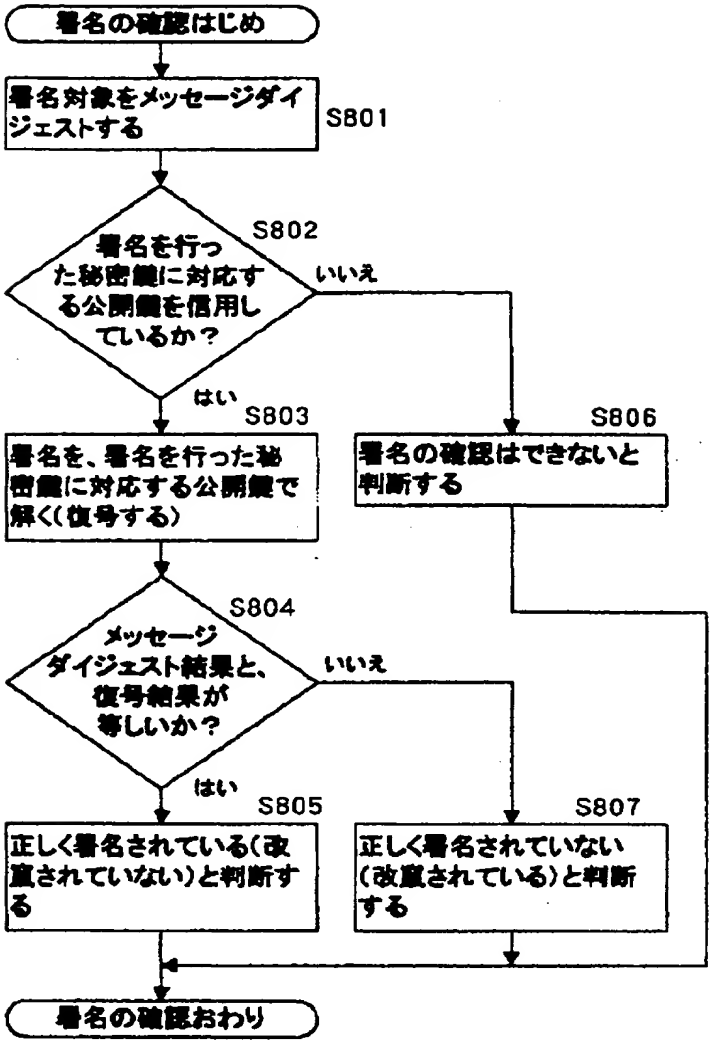
【図13】



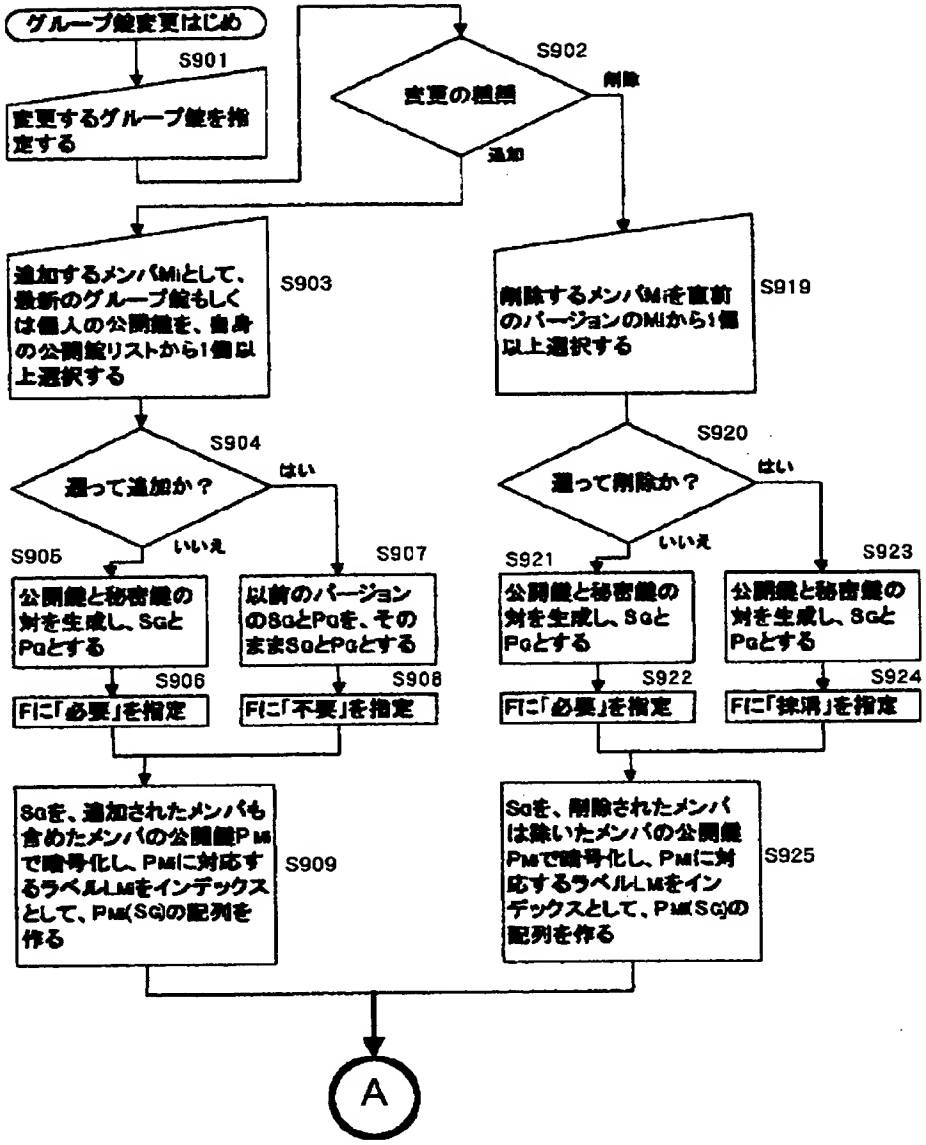
【図14】



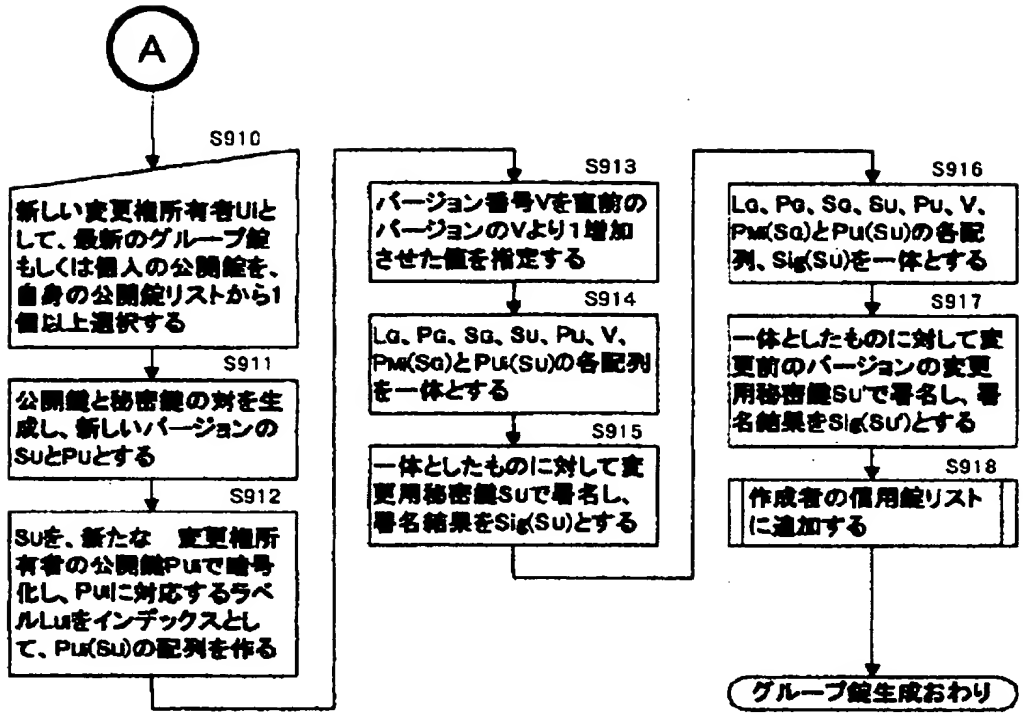
【図15】



【図16】



【図17】



フロントページの続き

(51)Int.Cl.⁶	識別記号	FI	
H04L 9/08		H04L 9/00	601F
			601A